UNCLASSIFIED

JADS JT&E-TR-99-012

JADS JT&E

JADS Special Report on Networking and Engineering

by: Charles P. Ashton, MSgt, USAF

August 1999

Distribution A - Approved for public release; distribution is unlimited.

Joint Advanced Distributed Simulation
Joint Test Force
2050A 2nd St. SE
Kirtland Air Force Base, New Mexico 87117-5522

UNCLASSIFIED

UNCLASSIFIED

JADS JT&E-TR-99-012

JADS SPECIAL REPORT ON NETWORKING AND ENGINEERING

19 August 1999

Prepared by: CHARLES P. ASHTON, MSgt, USAF
Wide Area Network Systems Engineer

Reviewed by: JAMES M. MCCALL, Lt Col, USAF
Chief of Staff, Air Force Deputy

Approved by: Mark E Smith
MARK E. SMITH, Colonel, USAF
Director, JADS JT&E

DISTRIBUTION A - Approved for public release; distribution is unlimited.

JOINT ADVANCED DISTRIBUTED SIMULATION
JOINT TEST FORCE
2050A 2nd St. SE
Kirtland Air Force Base, New Mexico 87117-5522

UNCLASSIFIED

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	19 Aug 99	15 Jun 95 - 30 Jul 99

4. TITLE AND SUBTITLE

JADS Special Report on Networking & Engineering, Appendices A, B, C, D, & E

5. FUNDING NUMBERS

N/A

6. AUTHOR(S)

CHARLES P. ASHTON, MSgt, USAF

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

JOINT ADVANCED DISTRIBUTED SIMULATION (JADS) JOINT TEST FORCE(JTF)
2050A 2nd St. SE
Kirtland Air Force Base, New Mexico 87117-5522

8. PERFORMING ORGANIZATION REPORT NUMBER

JADS JT&E-TR-99-012

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

OUSD(A&T) DD, DT&E
Deputy Director, Developmental Test and Evaluation
RM 3D1080
3110 DEFENSE PENTAGON
WASHINGTON DC 20301-3110

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

N/A

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

DISTRIBUTION A - APPROVED FOR PUBLIC RELEASE; DISTRIBUTION IS UNLIMITED.

12b. DISTRIBUTION CODE

DISTRIBUTION A UNLIMITED

13. ABSTRACT ***(Maximum 200 Words)***

The Joint Advanced Distributed Simulation (JADS) Joint Test Force (JTF) was chartered by the Office of the Secretary of Defense to investigate the utility of advanced distributed simulation (ADS) technology for test and evaluation (T&E). JADS executed three test programs; command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR), precision guided munitions, and electronic warfare, representing slices of the overall T&E spectrum as well as observing other activity within the T&E community to form its conclusions. Each of the three tests required that T&E facilities be linked together through a communications network to support an ADS architecture. While facility linking does not require cutting edge communications technologies, there are many tasks that must be carried out before successful ADS testing can begin. This report outlines the network design requirements, network description, and describes the components of the JADS communications network. Also, this report addresses JADS JTF costs, concerns and constraints, and lessons learned. It is intended to provide insight into the process JADS JTF undertook in setting up distributed communications networks capable of supporting ADS testing.

14. SUBJECT TERMS	15. NUMBER OF PAGES
	134
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UNLIMITED

Contents

Appendices

List of Figures

List of Tables

1.0 Purpose and Background

1.1 Purpose

This report describes the Joint Advanced Distributed Simulation (JADS) Joint Test Force (JTF) communications network. It outlines the network design requirements, network description, and describes the components. Also, this report addresses JADS JTF costs, concerns and constraints, and lessons learned. It is intended to provide insight into the process JADS JTF undertook in setting up a distributed communications network capable of supporting advanced distributed simulation (ADS) testing.

1.2 Background

The JADS Joint Test and Evaluation (JT&E) was chartered by the Deputy Director, Test, Systems Engineering and Evaluation (Test and Evaluation), Office of the Under Secretary of Defense (Acquisition and Technology) in October 1994 to investigate the utility of ADS technologies for support of developmental test and evaluation (DT&E) and operational test and evaluation (OT&E). The program is Air Force led with Army and Navy participation.

The JADS JTF is directly investigating ADS applications in three slices of the test and evaluation (T&E) spectrum: the Systems Integration Test (SIT) explored ADS support of air-to-air missile testing; the End-to-End (ETE) Test investigated ADS support for command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) testing; and the Electronic Warfare (EW) Test explored ADS support for EW testing. Each test applied the JADS objectives and measures as appropriate to conduct its evaluation.

1.2.1 Systems Integration Test (SIT) Description

The SIT evaluated the utility of using ADS to support cost-effective testing of an integrated missile weapon/launch aircraft system in an operationally realistic scenario. The SIT also evaluated the capability of the JADS Test Control and Analysis Center (TCAC) to control a distributed test of this type and to remotely monitor and analyze test results. The SIT consisted of the Linked Simulators Phase (LSP) and the Live Fly Phase (LFP). The missions simulated a single shooter aircraft launching an air-to-air missile against a single target aircraft. The LSP incorporated a manned F-18 avionics lab (simulator) at China Lake Naval Air Station (NAS) California, as the shooter; a manned F-14 avionics lab (simulator) at Point Mugu NAS California, as the target; and a missile hardware-in-the-loop (HWIL) simulation lab (simulator) at China Lake NAS which generated air intercept missile (AIM)-9 missile flyouts and injected countermeasures (flares). The LFP employed an architecture which incorporated a live F-16 shooter aircraft, a live F-16 target aircraft, and an Advanced Medium Range Air-to-Air Missile (AMRAAM) HWIL simulator hosted in the Eglin Air Force Base (AFB), Florida, Missile Lab.

1.2.2 End-to-End (ETE) Test Description

The ETE Test was designed to evaluate the utility of ADS to support testing of C4ISR systems. The test used the developmental and operational testing issues for the Joint Surveillance Target Attack Radar System (Joint STARS) in an ADS-enhanced environment to conduct its T&E utility evaluation. Also, the ETE Test evaluated the capability of the JADS TCAC to control a distributed test and remotely monitor and analyze test results. The ETE Test consisted of four phases. Phase 1 developed or modified the components that allowed a mix of live and simulated targets at an E-8C operator's console and a light ground station module (LGSM) operator's console. Phase 2 evaluated the utility of ADS to support DT&E and early OT&E of a C4ISR system in a laboratory environment. Phase 3 moved portions of the architecture to the E-8C aircraft, ensured that the components functioned properly, and confirmed that the synthetic environment interacted properly with the aircraft and actual LGSM. Phase 4 evaluated the ability to perform test and evaluation of the E-8C and LGSM in a synthetically enhanced operational environment using typical operators.

1.2.3 Electronic Warfare (EW) Test Description

The EW Test was designed to evaluate the utility of ADS in a distributed EW environment. It consisted of three phases. Phase 1 consisted of open air range and hardware-in-the-loop testing to develop a performance baseline for the two subsequent phases. Phase 2 employed a linked architecture that utilized the Department of Defense's (DoD) high level architecture (HLA) and included a digital system model of the ALQ-131 self-protection jammer, threat simulation facilities, and constructive models that replicated the open air environment. Phase 3 substituted an installed systems test facility (anechoic chamber) with an ALQ-131 pod mounted on an F-16 for the digital systems model. Both Phase 2 and Phase 3 compared system performance data with live fly data from Phase 1 for verification and validation (V&V).

2.0 Network Design Requirements

The network design requirements are broken into four distinct areas: common, SIT, ETE Test and EW Test requirements. The common network requirements were provided by the JADS Steering Committee (leadership). The individual test team requirements were provided by the JADS test teams.

2.1 Common Network Requirements

Although the three JADS JTF test programs were investigating the utility of ADS in distinctly different environments, the following were common requirements of the tests:

- Robust communications architecture with expansion capabilities.
- High reliability with the capability to remotely instrument performance of the communications circuits.
- Exclusive use and management of the bandwidth during periods of test or integration.
- Full control over scheduling of the network. It was determined that additional scheduling requirements increased the risk of conducting a test event. Also, the test teams had a need to respond to unscheduled availability of facilities for integration work.
- Complete management control of the communications network in order to make changes as needed and evaluate the performance of each link in the network.
- With the exception of the SIT, all links had to dedicate at least one 64 kilobits per second (Kbits) time slot for voice communications in support of test control and execution.
- National Security Agency (NSA)-approved communications security (COMSEC) equipment to encrypt the communications circuits.
- Routing equipment support for transmission control protocol (TCP)/internet protocol (IP) for data transmission.
- Routing equipment support for simple network management protocol (SNMP) in order to remotely instrument router performance.
- Routing equipment support for forwarding user datagram protocol (UDP) among all sites.

2.2 Systems Integration Test (SIT) Network Requirements

The SIT network had to support the following:

- Directed broadcasting of distributed interactive simulation (DIS) protocol data units (PDUs).
- Data rates between sites up to 768 Kbits.
- Closed-loop interaction, one-way latency less than 100 milliseconds (ms).
- Open-loop no interaction, one-way latency less than 300 ms.
- 10 megabits per second (Mbps) Ethernet to interconnect the various workstations and router at a site.
- If feasible, use existing network capabilities among sites.

2.3 End-to-End (ETE) Test Network Requirements

The ETE Test network had to support the following:

- Directed and selective broadcasting of DIS PDUs.
- The ability to transmit DIS PDUs from an unclassified network into a classified (secure) network environment.
- Data rates among sites up to 1024 Kbits.
- 10 Mbps Ethernet to interconnect the various workstations and router at a site.

2.4 Electronic Warfare (EW) Test Network Requirements

The EW Test network had to support the following:

- IP multicasting among all sites.
- One-way application-to-application latency less than 150 ms (300 ms round trip).
- Data rates among sites up to 1 Mbps.
- 10/100 Mbps Ethernet to interconnect the various workstations and router at a site.

3.0 Network Descriptions

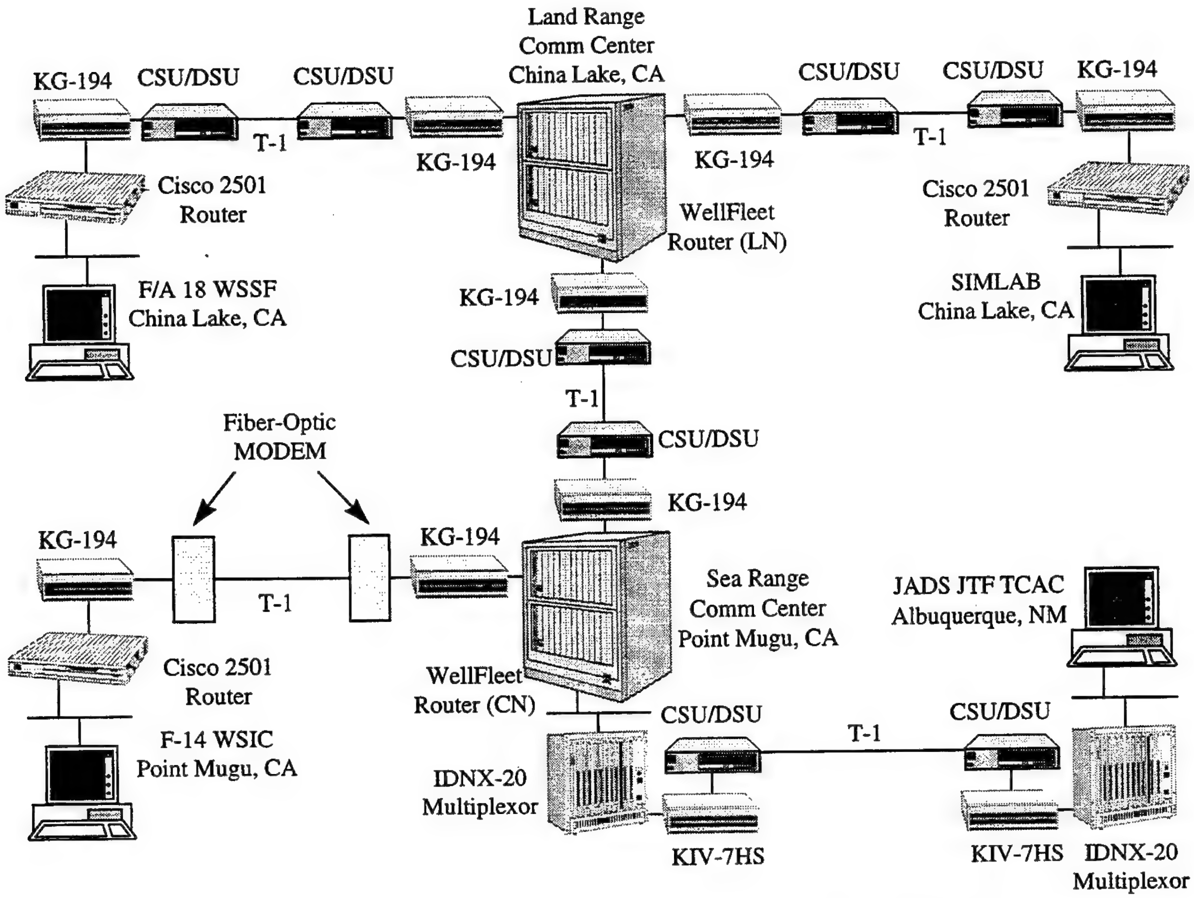
The following sections describe the individual JADS test teams' wide area networks (WAN). The figures represent an overview of the individual WANs and do not depict the network interface units (NIUs), simulators, or local area network (LAN) equipment at each site. Refer to Appendix A for detailed network diagrams.

3.1 Systems Integration Test (SIT)

The SIT was able to utilize existing networking infrastructure for both LSP and LFP. Also, JADS JTF was able to utilize the same networking equipment as the ETE Test and EW Test programs to connect the TCAC in Albuquerque, New Mexico, to the existing networks in Point Mugu and Eglin AFB.

3.1.1 Linked Simulators Phase

Figure 1 details the SIT LSP communications network. The involved facilities at Point Mugu and China Lake were already linked together through the Naval Air Warfare Center Weapons Division (NAWC-WPNS) Near-Real-Time Network (NRNet) at Point Mugu. JADS JTF leased a T-1 line from Albuquerque to Point Mugu and connected into the NRNet at the Sea Range Communications Center. Although the NRNet was pre-existing, it required extensive changes to the routers' configurations (directed broadcasting, routing tables, etc.) to support the SIT networking requirements. These modifications were primarily necessary because of differences in the various models and vendors of the routing equipment. Also, because of latency concerns and NRNet traffic loading, the missile simulator and F/A-18 labs at China Lake had to connect their military standard (MIL STD) 1553B data busses via a separate data circuit in order to get proper interaction between the F/A-18 weapons control system and the missile launch control system.

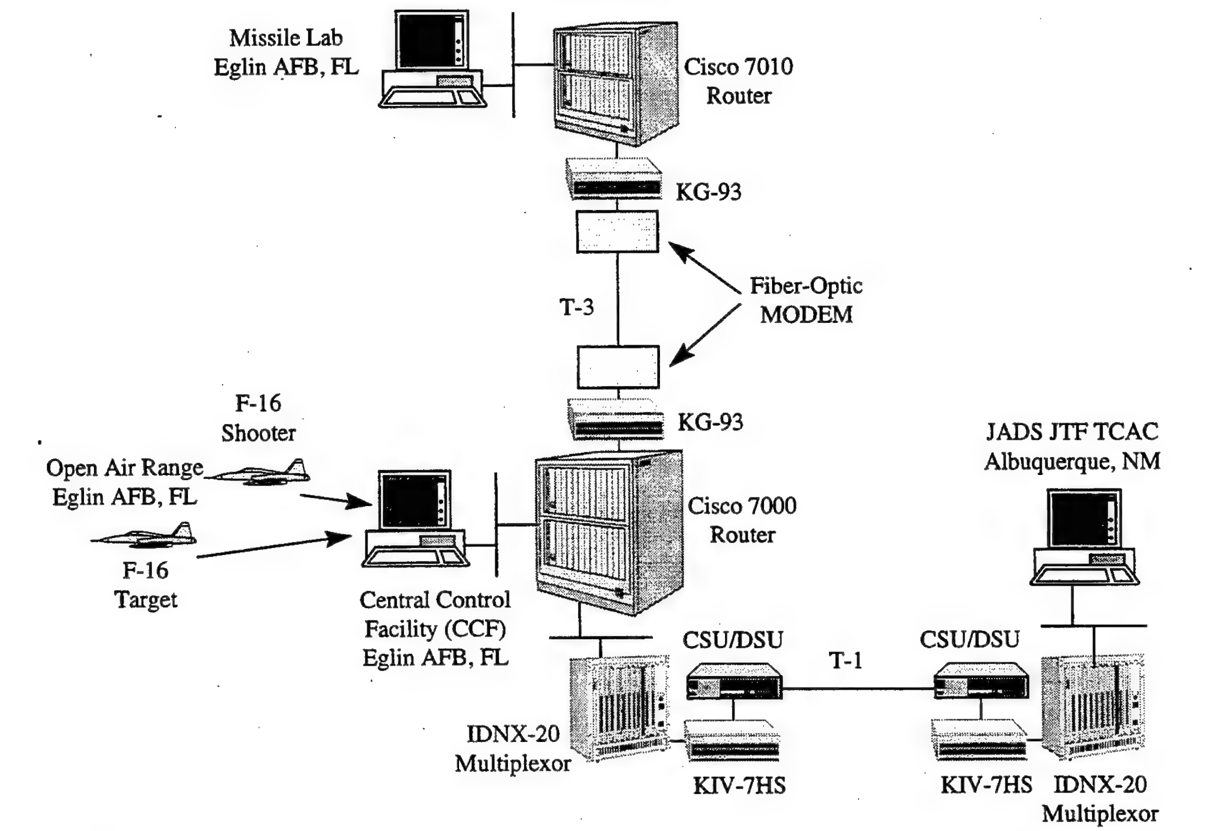


CSU = channel service unit
DSU = data service unit
INDX™ = Integrated Digital Network Exchange
KG = a family of communications security equipment
modem = modulator/demodulator
SIMLAB = Simulation Laboratory
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
WSIC = Weapons System Integration Center
WSSF = Weapon System Support Facility

Figure 1. SIT Linked Simulator Phase Network

3.1.2 Live Fly Phase

Figure 2 details the SIT LFP communications network. The involved facilities at Eglin AFB built a network infrastructure to meet the SIT LFP requirements. JADS JTF leased a T-1 line from Albuquerque to Eglin AFB and connected into Eglin's network at the Central Control Facility (CCF). The network required minor changes once all of the components were installed to optimize network performance and meet the LFP network requirements. The infrastructure and networking equipment at Eglin AFB were left in place as a legacy network for future ADS testing at Eglin AFB.

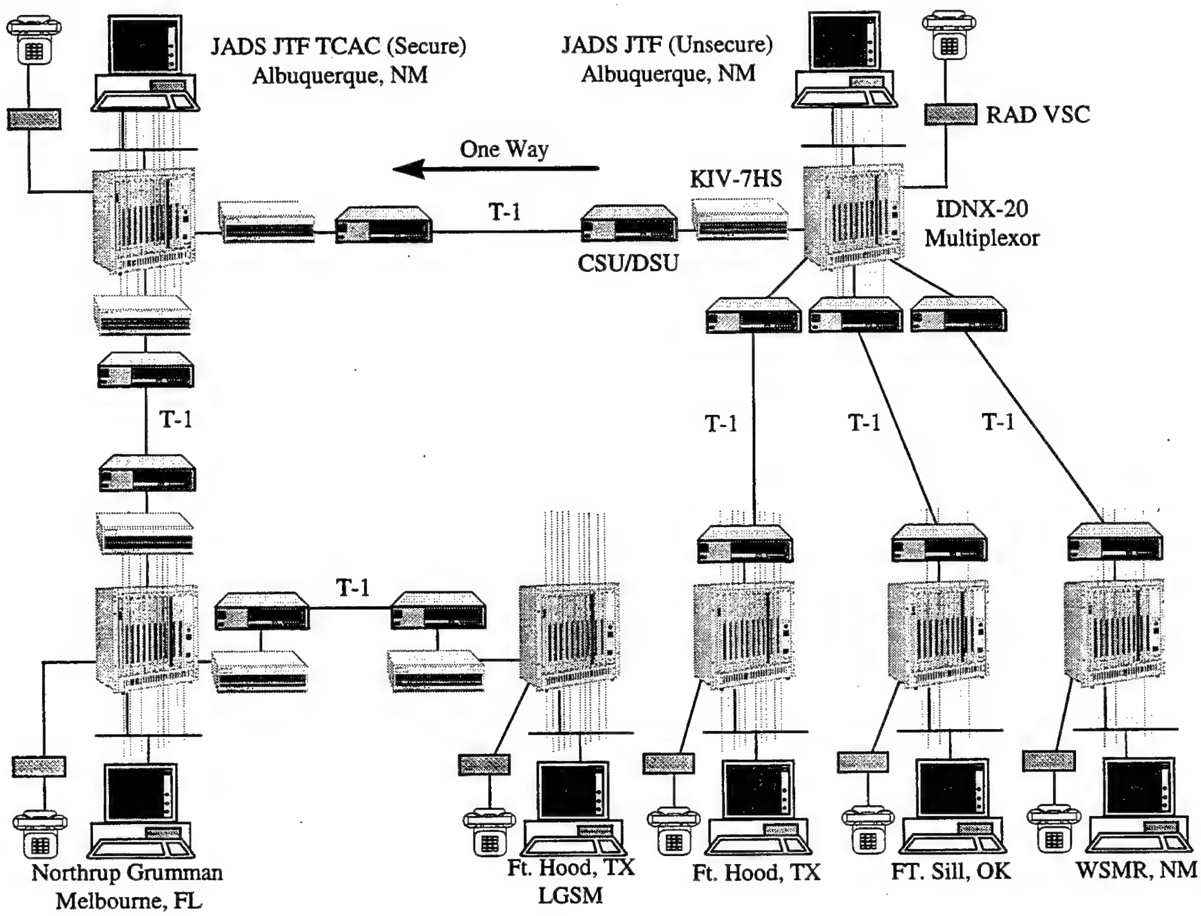


CSU = channel service unit
DSU = data service unit
INDX™ = Integrated Digital Network Exchange
KG = a family of communications security equipment
modem = modulator/demodulator
T- = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
T-3 = 28 T-1 lines in one; the aggregate data rate is 44.746 megabits per second

Figure 2. SIT Live Fly Phase Network

3.2 End-to-End (ETE) Test

Figure 3 details the ETE Test communications network. The ETE Test presented the challenge of transmitting UDP data from an unclassified site into a classified network. This was accomplished by configuring a one-way only link at the JADS facility. JADS JTF received unclassified (nonsecure) data from White Sands Missile Range (WSMR), New Mexico, and Fort Sill, Oklahoma, and forwarded these data into the TCAC, and prevented any data from the secure network propagating to the nonsecure network.

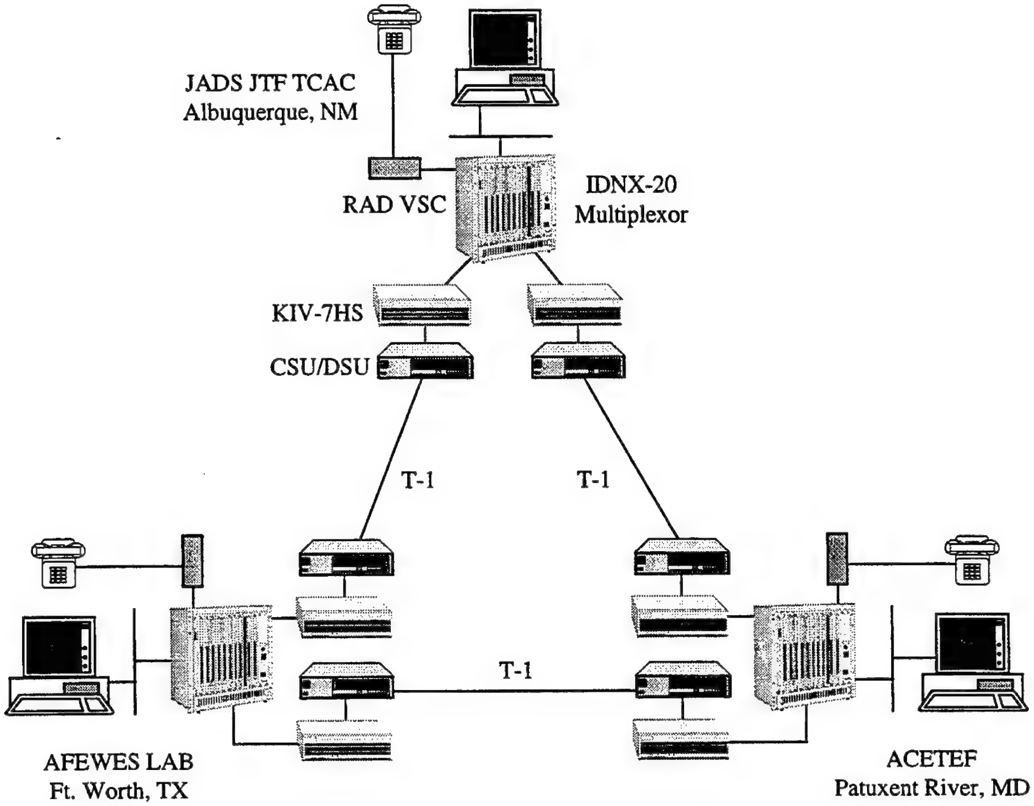


CSU = channel service unit DSU = data service unit INDX™ = Integrated Digital Network Exchange
KIV = AlliedSignal embeddable KG-84 communications security
RAD = the company that manufactures the voice signal converter
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second VSC = voice signal converter

Figure 3. ETE Test Network

3.3 Electronic Warfare (EW) Test

Figure 4 details the EW Test communications network. The EW Test presented many challenges in the networking equipment configuration. Although the EW Test was able to utilize the same equipment as the SIT and the ETE Test, the network equipment required extensive configuration changes to optimize the routers' performance while reducing transmission latency to minimal levels.



ACETEF = Air Combat Environment Test and Evaluation Facility
AFEWES = Air Force Electronic Warfare Evaluation Simulator
CSU = channel service unit
DSU = data service unit
INDX™ = Integrated Digital Network Exchange
KIV = AlliedSignal embeddable KG-84 communications security
RAD = the company that manufactures the voice signal converter
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
VSC = voice signal converter

Figure 4. EW Test Network

4.0 Equipment Descriptions

The JADS JTF communications network can be broken down into three distinct segments: the LAN, the WAN, and the Clock Distribution System (CDS). This section will describe the networking equipment installed by the JADS JTF, even though NRNet and Eglin AFB used equipment from other vendors.

4.1 Local Area Network

A variety of LAN technologies were used to support the three JADS JTF test programs. The LANs mainly consisted of hubs and switches. However, Eglin AFB employed a combination of 10 Mbps Ethernet and fiber-optic distributed data interfaces (FDDI). To the extent possible, the LANs contained only equipment directly supporting the JADS tests. This was achieved at all sites except the F-14 Weapons System Integration Center (WSIC) during the SIT LSP. A bridge was used to isolate the JADS equipment from the rest of the WSIC LAN.

4.1.1 Hubs

The hubs were used to interconnect the various computer workstations and the router at a site. JADS JTF utilized a variety of unintelligent 10 Mbps half-duplex Ethernet hubs that were available from multiple vendors.

4.1.2 Switches

The switches were used in the same manner as the hubs to interconnect the computer workstations and the router at a site. The main difference between a switch and a hub is that a switch will selectively route data that its workstations operate at 100 Mbps full-duplex. In order to accommodate this requirement, JADS JTF implemented 10/100Base-T auto-sensing switches that were available from multiple vendors.

4.2 Wide Area Network

Although it was not a requirement, it was desirable to utilize commercial-off-the-shelf (COTS) equipment that was easily obtainable and reasonably affordable. JADS JTF procured all of the WAN equipment through government contracts with significant cost savings compared to the vendors' list prices.

4.2.1 Channel Service Unit/Data Service Unit

The channel service unit (CSU)/data service unit (DSU) interfaces the KIV-7HS encryption device or the Integrated Digital Network Exchange (IDNX™) trunk module to the T-1 communications line by converting the non-return to zero (NRZ) output of the KIV-7HS to a bipolar alternate mark inversion (AMI) signal for transmission over the telecommunications carrier facilities. In addition, the CSU/DSU supports binary eighth zero substitution (B8ZS)

encoding and inserts framing bits in the extended super frame (ESF) format. Also, the model (VERILINK AS2000) of CSU/DSU used by the test networks was capable of remote configuration management and monitoring.

4.2.2 KIV-7HS Encryption Device

The KIV-7HS is a NSA-certified link encryption device used to protect the data being transferred between sites. The KIV-7HS protects classified and sensitive digital data transmissions (Type I) at data rates up to 1.544 Mbps. Its performance characteristics are similar to the KG series of cryptographic equipment. The KIV-7HS supports the T-1 data rate with one-way, end-to-end latency of 4.5 microseconds. Also, the primary reason JADS JTF utilized the KIV-7HS was the significant cost savings over the KG series of encryption device. The cost of installing a pair of KIV-7HS encryption devices on a communications circuit was $7,969 versus $20,800 to install a pair of KG-194 encryption devices.

4.2.3 Integrated Digital Network Exchange

IDNX™ is a communications resource manager (CRM), or multiplexer, that supports and integrates a broad range of voice, data, and internetworking services. The entire network can be monitored, managed and controlled from any IDNX™ node in the network. JADS JTF chose the IDNX™-20 series of CRM because of these features and the IDNX™ family of products is extensively used by the Defense Information Systems Agency (DISA) in support of the Defense Information Systems Network (DISN). The ability to configure and manage the systems allowed JADS to quickly troubleshoot problems and reconfigure the network equipment to meet test team requirements. The following subsections only describe the feature modules utilized by the JADS JTF.

4.2.3.1 I422 Trunk Card

The I422 trunk card provides an RS-449/422 compatible interface for the IDNX™ to interface with the KIV-7HS or the CSU/DSU (nonsecure applications). The module also contains a crypto sync relay that allows it to support automatic external resynchronization of encryption equipment. The I422 trunk module does real-time multiplexing, synchronization, inter-nodal signaling, and contains the logic to control allocation of trunk channels. It allocates 16 Kbits of the T-1 bandwidth to an inter-nodal communications channel which is the sole means by which nodes communicate with one another. The channel carries data that allow the network manager to configure, query, and monitor all nodes from anywhere in the network. The inter-nodal channel provides

- Call processing, configuration, network events, and status information to all nodes in the network.
- Code loading when the desired code is not present in the node.
- Database information, events, alarms, and circuit management messages to the network manager.
- Continuous bit error rate test (BERT) in 30 minute intervals on the communications circuit .

4.2.3.2 PX-3 and Access PX Router Modules

The packet exchange (PX) platform is a general purpose router/bridge module integrated into the IDNX™ CRM. The PX platform provides packet-switched services among LANs over a wide area network through the IDNX™ CRM. The module connects the LAN to the WAN via an Ethernet (Institute of Electrical and Electronics Engineers [IEEE] 802.3) or switchable 4/16 Mbps token ring (IEEE 802.5) interface. The PX platform features an onboard processor and up to eight high-speed serial ports. PX platform serial ports can be connected to remote PX modules or to local or remote data cards with external serial ports. The access PX (access packet exchange [APX]) module was used to support the ETE Test and both phases of SIT. The APX utilizes Cisco release 9.1(9) for its operating system. Also, the APX is not year 2000 (Y2K) compliant and does not support IP multicasting. The PX-3 module was implemented for the EW Test. The PX-3 module utilizes Cisco release 11.1 for its operating system. In addition, the PX-3 module supports IP multicasting and is Y2K compliant. JADS JTF used the APX module for the SIT and the ETE Test because the PX-3 module was not available from the vendor at test equipment procurement time.

4.2.3.3 Quad Analog Voice Processor Module

The quad analog voice processor (QAVP) module provides and manages voice calls coming into and leaving the WAN. It serves as the interface between external voice communications equipment and the rest of the network. The QAVP module supports four full-duplex channels, which connect to industry standard 4-wire E&M analog communications equipment. The module converts 3 kilohertz (kHz) bandwidth analog signals to 64 Kbits digital pulse code modulation (PCM) and vice versa. It features echo cancellation, which eliminates echo caused by hybrid transformers that connect two-wire circuits with analog four-wire circuits.

4.2.4 RAD Voice Signal Converter

The RAD voice signal converter (VSC) interfaces between an ordinary 2-wire telephone set and the 4-wire E&M interface enabling direct connection to the analog interface of a time division multiplexer. The VSC recognizes the telephone set pulses for on hook, off hook and dialing, translates the pulses into the proper signaling standard, and sends the resulting signal over the "M" lead. When detecting activity on the "E" lead, the VSC sends the ring signal to the telephone and the ring back tone to the 4-wire E&M interface of the QAVP.

4.3 Clock Distribution System (CDS)

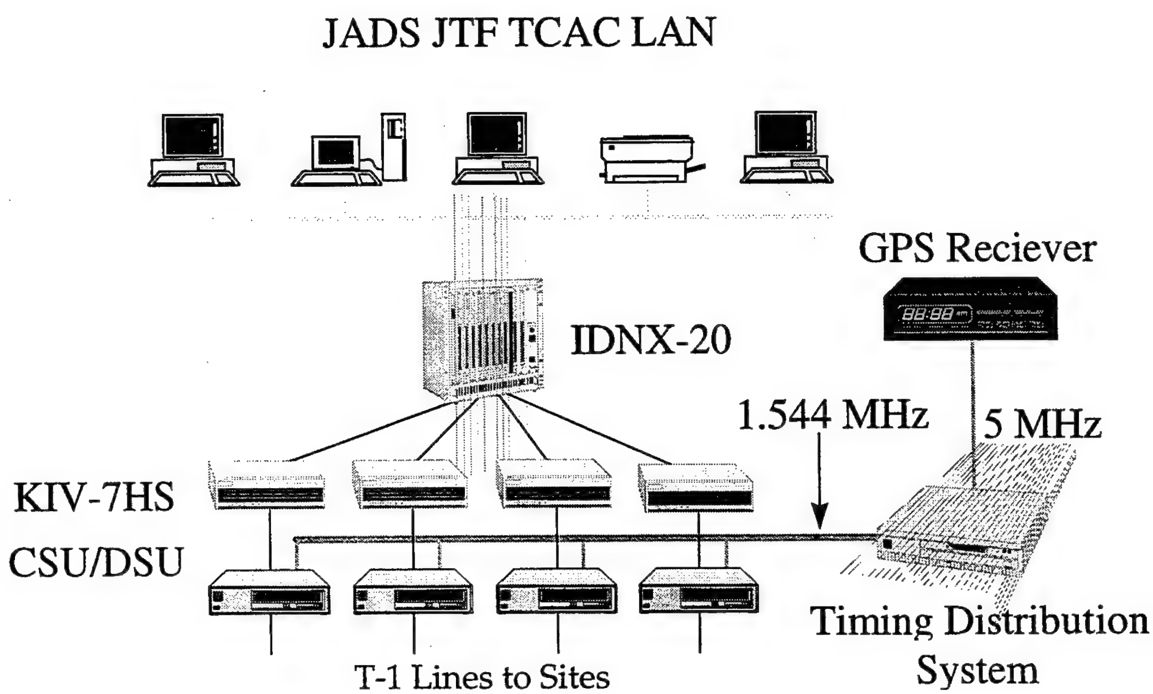
The CDS was used to synchronize all of the WAN equipment to the same timing source. It is vital that the network be slaved to the same timing signal in order to maintain synchronization and prevent bit errors caused by differences in timing in the WAN equipment. The CDS is comprised of three components: the true-time Global Positioning System (GPS) receiver, Fiber Plex Timing Distribution System (TDS), and the CSU/DSUs. Figure 5 depicts how the timing signals were distributed among all the JADS test networks.

4.3.1 True-Time Global Positioning System Receiver

The GPS receiver is a stratum level 1 time source that is provided by the GPS satellite constellation. It has 1 megahertz (MHz), 5 MHz, and 10 MHz signal outputs for use by TDSs. JADS used the 5 MHz signal as the master frequency for input to the TDS.

4.3.2 Fiber Plex Timing Distribution System (TDS)

The Fiber Plex TDS was used to provide and distribute precision local timing to synchronous communications equipment. The TDS accepts the precision timing signals from the GPS receiver and phase locks a local oscillator to the signal. The local oscillator then divides the input frequency down to frequencies usable by the communications equipment. These outputs were wired directly to the external timing inputs of the CSU/DSUs. Then, the CSU/DSUs at the distant sites derived their timing from the incoming data stream from JADS. Figure 5 shows how JADS JTF utilized the CDS.



KIV = AlliedSignal embeddable KG-84 communications security
T-1 = digital carrier used to transmit a formatted digital signal at 1.544 megabits per second

Figure 5. Clock Distribution System

5.0 Network Instrumentation Tools

As part of the requirements definition process, it was deemed essential to evaluate the impact of network performance on test execution. A variety of commercially available tools were evaluated for the capability to perform pretest, real-time, and post-test analysis to evaluate performance of the various test networks and their impact on the quality of collected test data. The network performance areas of primary interest were latency, bandwidth utilization, and data losses. The following sections describe the network instrumentation tools JADS used in evaluating network performance.

5.1 Silicon Graphics, Inc., (SGI) *NetVisualyzer™*

NetVisualyzer™ is a network analysis package developed by Silicon Graphics Inc. This product is a suite of protocol analysis tools that can be used during network setup or during testing to ensure that network equipment is configured properly, nodes are talking to one another as intended, and to assist the network manager in identifying, eliminating, or minimizing extraneous network traffic. Remote data stations, located on each LAN segment, collect data and send them to a central display station, where the information is processed by the individual analysis tools and graphically displayed. The additional network load caused by the active data collection over the network was found to be negligible during ETE testing. Traffic flow among specific hosts at each site and among sites is shown near real time, enabling test controllers to quickly realize if link availability among sites is compromised. The ability to monitor current packet rate and load at the LAN level, a valuable asset in evaluating tactical system or simulation activity at an individual site, is offered by another piece of the *NetVisualyzer™* tool set.

5.2 Cabletron *SPECTRUM®*

SPECTRUM® is a network analysis package developed by Cabletron Systems. It provides a near real-time capability for network traffic monitoring, presenting current packet rate and load information, as well as packet error and discard rate information for network equipment. The package also provides an alarm manager with simple diagnostic capability that is valuable in the detection and troubleshooting of network outages. *SPECTRUM®* utilizes the Simple Network Management Protocol (SNMP) to periodically query network devices and displays requested information on screen in table and graphical format. The *SPECTRUM®* operator can tailor the destination, frequency, and content of the queries to provide the desired level of insight into a particular network portion or piece of equipment. Like *NetVisualyzer™*, *SPECTRUM®* queries for data to create network traffic, although not of appreciable quantity to be noticed in relation to the test traffic. Typically, a five-second polling interval was used to monitor the network equipment, a value chosen so that short duration problem events would most likely not be missed. Multiple databases store *SPECTRUM®'s* event log and query results for later analysis.

5.3 AG Group, Inc., *EtherPeek™*

EtherPeek™ is a network analysis package developed by AG Group Inc. This product is a suite of protocol analysis tools that can be used during network setup or during testing to ensure that network equipment is configured properly, nodes are talking to one another as intended, and to assist the network manager in identifying, eliminating, or minimizing extraneous network traffic. It provides real-time capability for network traffic monitoring, presenting current packet rate and load information, as well as packet error information. Local and remote *EtherPeek™* data stations passively collect all LAN traffic at each site for real-time network analysis. Unlike *NetVisualyzer™* and *SPECTRUM®*, *EtherPeek™* does not create any additional network traffic. The protocol analysis part of the tool set was extremely valuable to the EW Test in analyzing latency and data dropouts between nodes.

6.0 Cost

The costs involved in setting up a communications network can be presented a number of different ways. No matter how they are presented, there are two underlying constants that must be accounted for in planning a network. These are communications hardware and circuit costs. A JADS communications node consisted of an IDNX™ CRM, KIV-7HS encryption device, and a CSU/DSU. On average, JADS typically expended approximately $36,000 per site and approximately $90,000 to set up a central communications facility. Communication circuit costs mainly depend upon distance between sites and tariffs imposed by the service provider. Table 1 lists the costs JADS incurred to initially install a circuit (nonrecurring charge or NRC) and the monthly fee thereafter (monthly recurring charge or MRC).

Table 1. Circuit Cost Information

Origination	Destination	NRC	MRC
SIT			
Albuquerque, NM	Point Mugu, CA	$3,763.00	$3,448.00
Albuquerque, NM	Eglin AFB, FL	$2,313.00	$4,604.00
ETE Test			
Albuquerque, NM	WSMR, NM	$0	$700.00
Albuquerque, NM	Fort Sill, OK	$2,500.00	$2,900.00
Albuquerque, NM	Fort Hood, TX	$2,300.00	$3,300.00
Albuquerque, NM	Melbourne, FL	$2,800.00	$4,600.00
Melbourne, FL	Fort Hood, TX	$3,400.00	$3,800.00
EW Test			
Albuquerque, NM	Patuxent River, MD	$1,059.00	$5,527.00
Albuquerque, NM	Fort Worth, TX	$2,457.00	$2,985.00
Ft. Worth, TX	Patuxent River, MD	$1,832.00	$4,873.00

7.0 Concerns and Constraints

7.1 Requirements Definition

Network requirements (i.e., expected data rate, latency budget, communications protocols, control and management of the network) need to be defined early in the process. These requirements must be clearly defined and forwarded to DISA for evaluation of how they can best support the requirements, either through DISA common user networks (i.e., Defense Simulation Internet (DSI), Secret Internet Protocol Router Network (SIPRNET), Defense Research and Engineering Network (DREN), etc.) by granting a waiver exempting use of common user networks in order to build a private network suitable for the requirements. An overview of the different DISA common user networks is contained in Appendix B. It should be noted that if DISA's common user networks are to be used, DISA will allow connection to only one of the networks. These networks cannot be interconnected because of security, interoperability, and tariff constraints. Thus, it requires close coordination with DISA to ensure the network of choice will support all requirements. Network performance data concerning DSI, DSI asynchronous transfer mode (ATM) backbone, and SIPRNET are contained in Appendixes B, C, D, and E.

7.2 Cost

Cost becomes a factor depending upon the networking solution or waiver provided by DISA. The cost of using one of DISA's common user networks may be too high for some customers, depending on which network DISA suggests will meet the requirements. For example, there is a one time NRC of $64,000 to join the DSI with a monthly recurring charge (MRC) of $9,000 per T-1 circuit. Table 2 shows the charges associated with joining SIPRNET. For both networks, the NRC included procurement, installation, and configuration of all necessary equipment. The MRC included operation, configuration management, and maintenance of all equipment and circuits. However, in the case of SIPRNET, the NRC only provided for installation of a central node. Any equipment and/or costs to extend service from that node are the responsibility of the customer.

Table 2. SIPRNET Costs

All Theaters IP Router Service - Monthly Recurring Charges / Fiscal Year 98

Bandwidth:	Ethernet	9.6kB	19.2kB	*56/64kB	128kB	256kB	512kB	1024kB-T-1	E1
Continental United States (CONUS)	$7,748	$1,033	$1,033	$1,033	$1,808	$3,099	$5,165	$6,198	N/A
EUROPE	$10,304	$1,288	$1,288	$1,228	$2,254	$3,864	$6,440	$7,728	$8,372
PACIFIC (HA/AL)	$7,748	$1,033	$1,033	$1,033	$1,808	$3,099	$5,165	$6,198	N/A
PACIFIC RIM	$10,800	$1,350	$1,350	$1,350	$2,363	$4,050	$6,750	$8,100	N/A

*56 kilobytes (kB) available in continental United States (CONUS), 64 kB available for outside the CONUS connectivity.

**NRC for installations: $2,500 for less than 512 Kbits and $5,000 for greater than or equal to 512Kbits.

***Dial-up service equals $50 initiation fee plus $27 per month per comm server access card.

****Dual homing - Second connection of dual homed system will be charged 50% of the MRC that the second connection line speed would ordinarily prompt.

*****The management of customer premise routers (Cisco or Wellfleet routers) have a flat fee of $50 per month for all new customers. All other router management (not Cisco or Wellfleet) will require a specific cost estimate to determine a fee.

7.3 Time

Time is of the essence. Careful planning and consideration must be given to the schedule for implementing the communications network. On average, once the requirements are defined and a networking solution is decided upon, it will take a minimum of 120 days (if a DISA common user network is to be utilized, it could take more than 180 days) to procure and install the necessary communications circuits and networking hardware. Also, it will take a minimum of 90 days to obtain the necessary COMSEC equipment and keying material to encrypt the data. It may take longer if a COMSEC subaccount needs to be established. In addition, time must be allocated in the schedule to install, test, and validate communications network performance. On average, JADS allocated one week per site to accomplish these tasks.

8.0 Lessons Learned

8.1 Planning and Requirements Definition

1. The requirements for an ADS test must be clearly defined early in the test planning phase. Detailed planning and coordination will be required to ensure a common understanding of all requirements, procedures, test objectives, etc., since individual facilities are not generally familiar with conducting coordinated, distributed T&E tests.

2. Network experts must be involved from the beginning. There should be more than one expert, and they must be involved from the beginning of the project to establish the data and instrumentation requirements, verify/validate the networking approach, assist in the development of procedures, and provide overall system expertise.

3. Early definition of network requirements was very advantageous. Having accurate requirements for network connectivity identified early in the program was very advantageous for linking the distributed facilities. JADS network experts estimated the necessary data throughput, encryption, and storage requirements for the ADS network. Their accuracy and resourcefulness allowed them to choose among a few hardware and firmware alternatives, and their early decision making allowed enough time to acquire the right components through government channels and contracting of data circuits through the DISA. This early planning allowed early network integration testing, well ahead of other facility check-outs.

8.2 Network Security

Network security is an essential part of operating an ADS network. The network accreditation process needs to be addressed and started in the planning phase. Security and accreditation procedures are different for every site and branch of service. Hence, it becomes inherently difficult to execute interagency memorandums of agreement (MOA). Security focal points and designated approval authorities need to be identified early in the planning process, and close coordination with these individuals is essential to executing network installation and meeting test schedules. It is wise to factor approximately three months into the implementation schedule to execute the required security MOAs.

8.3 Impact of Network Protocols

8.3.1 User Datagram Protocol (UDP)

UDP is the protocol used by the distributed interactive simulation standard. Since UDP is a broadcast protocol, it is not normally forwarded outside of a LAN. Special consideration must be given to the expected flow of data and interactions among sites in an ADS network in order to properly configure the routing equipment to support the test.

8.3.2 IP Multicasting

IP multicasting is one of the protocols used by the DoD HLA. IP multicasting is a protocol designed to support the broadcasting of information to specific groups of hosts rather than to all hosts on the network. The EW Test used HLA to conduct both Phase 2 and Phase 3. Special consideration had to be given to the different types of data being transmitted during the test in order to determine which data types would be transmitted TCP/IP or IP multicast.

8.4 Network Instrumentation Tools

Network instrumentation tools potentially may have a negative impact on network performance. In particular, a sudden drop in packet rate picked up by Cabletron's *SPECTRUM®*, or an altered data traffic pattern on one of the SGI *NetVisualyzer™* graphs may indicate a network link problem. However, these tools necessarily create additional network traffic with data queries, changing the very nature of the network traffic as they are monitoring it. Taking advantage of the capabilities of simpler tools is one alternative to the trade-off between intrusive monitoring and the need for insight into performance. One nonintrusive solution makes use of the self-diagnostic capabilities of the network equipment. For ETE and EW testing, a line printer in the TCAC facility was set up to print the diagnostic messages directly from the IDNX™ CRM. The sound of the printer would draw immediate attention to a potential equipment outage without intrusive monitoring.

8.5 ADS Network Implementation Guidelines

There were many challenges in designing and implementing a network architecture to support ADS testing. The lessons culminated in the following process that JADS JTF recommends for the design of an ADS-capable network suitable for the T&E community. This section outlines the steps in implementing ADS-based network architecture from a networking point of view.

STEP 1: Define Requirements

Activity 1.1: Identify Sponsor Needs
- Describe critical systems of interest
- Identify resources available to support ADS implementation (e.g., funding, personnel, tools, facilities)
- Identify any known test constraints (e.g., due dates, security requirements)

Activity 1.2: Develop Objectives
- Develop an ADS architecture/network development plan including approximate schedule and major milestones
- Develop a configuration management plan
- Identify security requirements (e.g., classification level and designated approval authority)
- Determine if ADS implementation is appropriate. In general, ADS implementation is necessary if entities interact with each other and if linking is necessary to permit the interactions

- Determine ADS architecture requirements
  * Data requirements
    ◊ What data types must be exchanged to permit interaction
    ◊ What data are required to achieve test objectives
    ◊ Rates of data exchanged among entities (in bits per second)
      – Will data be sent out of the simulation interface at the same rate as received by the generating entity or will dead reckoning be used to reduce data rates over the WAN because of WAN bandwidth restrictions
    ◊ Data time stamp accuracy requirement
    ◊ Data classification and security handling requirements
  * Latency requirements
    ◊ Acceptable latency and latency variations
    ◊ Closed-loop interaction requirements
  * Data quality requirements
    ◊ Acceptable level of ADS-induced errors (e.g., dropout rate, missing PDUs)
    ◊ Data sources and amounts
  * Network requirements
    ◊ Protocols to be used
      – Decide whether to use standard protocols (e.g., DIS PDUs) or to keep data in formats generated by entities
    ◊ Will HLA be implemented. Using HLA will affect the choice of protocol and simulation interface design and requires an appropriate runtime infrastructure
    ◊ Will data from nodes be broadcast or transmitted point-to-point. HLA implementation is a factor in this determination
    ◊ Data encryption requirements based on classification of data to be passed over WAN
  * Test control and monitoring requirements
    ◊ Test control concept
      – Central control location
      – Test coordinator and location at each distributed node/facility
    ◊ Live entity control technique
      – Is local range control required because of safety considerations or policy
      – Is remote live entity control possible; determine monitoring/communications requirements
    ◊ Display and monitoring requirements
      – Monitoring status of entities
      – Monitoring status/performance of distributed network
    ◊ Voice communications requirements and adequacy of existing telephone systems

STEP 2: ADS Architecture Design

Activity 2.1: Design Architecture

- Determine location of nodes
  * Select simulation facilities based on fidelity, availability, cost, and schedule
  * For live shooter/target configurations, select test ranges based on instrumentation quality and quantity, data processing capability, availability, cost, and schedule
- Conduct surveys of each site (node location)
  * Determine facility communications architecture and requirements
  * Determine physical space requirements for tester-supplied equipment and personnel
- Determine security approach
  * Designate security point of contact
  * Perform security risk assessment and develop concept of operations
- Determine WAN bandwidth requirement
  * For average and maximum aggregate data rate, add rates from each entity broadcast over the WAN
  * Bandwidth requirement equals aggregate data rate plus a 50% - 100% margin for overhead and unanticipated traffic
- Select WAN and LAN
  * DoD-sponsored network or commercial leased lines
    ◊ Consolidate network requirements
      – Acceptable latency limits
      – Aggregate data rates
      – Network management/control
    ◊ Submit requirements to DISA/D36 for determination of whether DISN common user services (e.g., Defense Simulation Internet, SIPRNET) will support the requirements or if a waiver is justified
    ◊ If a waiver is justified, survey commercial line lease rates
      – Dedicated (full-time) leased lines or on-demand leased lines
      – Contract for leased lines
- Select network hardware
  * Type(s) of router(s), CSU/DSU, mulitplexers, etc.
    ◊ If possible, use same type of router for all nodes
    ◊ Router addressing scheme
  * Type(s) of encryptor(s)
- Select test control hardware and software
  * Communications requirements
    ◊ Data communications requirements
    ◊ Voice communications requirements
- Develop formalized plan for architecture development and integration

Activity 2.2: Develop Architecture

- Procure or develop network analysis/monitoring tools
  - ∗ Determine required extent of analysis/monitoring
    - ◊ Troubleshooting only versus collecting and analyzing data
    - ◊ Bandwidth monitoring
      - – All versus some links
      - – Monitor LANs locally versus remote
    - ◊ Hardware requirements (using simple network monitoring protocol)
      - – Communications monitoring hardware
  - ∗ Obtain permission to monitor or collect data
- Develop procedures for secure/encrypted operations and obtain designated approval authority approval for their use
  - ∗ Coordinate security memoranda of agreement with organizations involved
  - ∗ Accredit networks, facilities, rooms, etc.
  - ∗ Establish communications security account
  - ∗ Order keying material
- Implement strict hardware and software configuration control

STEP 3: ADS Architecture Integration and Test

Activity 3.1: Execution Planning

- Develop integration test plan which incrementally checks out configuration during build-up
  - ∗ Initially test each WAN link separately
    - ◊ First test at CSU/DSU level to make sure communications work at lowest level
    - ◊ Use ADS protocols to test routing
    - ◊ Use pings to check for connectivity and loading problems
    - ◊ Test simulation-to-simulation connections
  - ∗ Test simulation-to-simulation connections with all nodes on the network
    - ◊ Use network analysis/monitoring tools to troubleshoot the network
    - ◊ Use ADS protocols to test routing
- Develop test control procedures
- Develop detailed execution plans.
- For secure networks, develop security test and evaluation plan

Activity 3.2: Integrate and Test ADS Architecture

- Install network hardware and software
- Perform compliance testing
  - ∗ Test each facility/node individually to ensure that ADS capability and any required modifications (including software) have been correctly implemented
- Perform integration testing
  - ∗ Check out interfaces and facility modifications with linking between pairs of nodes
  - ∗ Baseline performance of network with no loading from the simulations/entities
  - ∗ Test performance of critical portions of network under loading representative of test conditions to be used

9.0 References

1. Systems Integration Test, Linked Simulators Phase, Final Report, Joint Advanced Distributed Simulation Joint Test and Evaluation, Albuquerque, New Mexico, July 1997

2. Systems Integration Test, Live Fly Phase, Final Report, Joint Advanced Distributed Simulation Joint Test and Evaluation, Albuquerque, New Mexico, March 1998

3. Integrated Digital Network Exchange Technical Documentation, Network Equipment Technologies, Copyright 1995

4. Voice Signaling Converter Installation and Operation Manual, RAD Data Communications Ltd., Copyright 1997

5. Users Manual, Timing Distribution Systems, Buffer Systems, Distribution Amplifiers, Fiber Plex Incorporated, 1997

6. The Utility of Advanced Distributed Simulation for Precision Guided Munitions Testing, Joint Advanced Distributed Simulation Joint Test and Evaluation, Albuquerque, New Mexico, May 1998

7. "Guidance for Complying with ASD(C3I) Policy, 5 May 97, Mandating Use of Defense Information Systems Network (DISN) or FTS Common User Telecommunications Services," HQ DISA message, DTG 121734Z Aug 97

10.0 Acronyms and Abbreviations

ACETEF	Air Combat Environment Test and Evaluation Facility, Patuxent River, Maryland; Navy facility
ADS	advanced distributed simulation
AFB	Air Force base
AFEWES	Air Force Electronic Warfare Evaluation Simulator, Fort Worth, Texas; Air Force managed with Lockheed Martin Corporation
AG	AG Group, Inc.
AIM	air intercept missile
ALQ-131	a mature self-protection jammer system; an electronic countermeasures system with reprogrammable processor developed by Georgia Technical Research Institute
AMI	alternate mark inversion
AMRAAM	advanced medium range air-to-air missile
APX	access packet exchange
ATM	asynchronous transfer mode
B8ZS	binary 8th zero substitution
BERT	bit error rate test
C4ISR	command, control, communications, computers, intelligence, surveillance and reconnaissance
CCF	Central Control Facility
CDS	Clock Distribution System
COMSEC	communications security
CONUS	continental United States
COTS	commercial off-the-shelf
CRM	communications resource manager
CSU	channel service unit
DIS	distributed interactive simulation
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DoD	Department of Defense
DREN	Defense Research and Engineering Network
DSI	Defense Simulation Internet
DSU	data service unit
DT&E	developmental test and evaluation
E&M	analog voice signaling standard
ESF	extended super frame
ETE	End-to-End Test
EW	Electronic Warfare Test
FDDI	fiber distributed data interface
GPS	global positioning system
HLA	high level architecture
HWIL	hardware-in-the-loop (system integration references)

IDNX™	Integrated Digital Network Exchange
IEEE	Institute of Electrical and Electronics Engineers
IP	internet protocol
JADS	Joint Advanced Distributed Simulation, Albuquerque. New Mexico
Joint STARS	Joint Surveillance Target Attack Radar System
JT&E	joint test and evaluation
JTF	joint test force
kB	kilobytes
Kbits	kilobits
KG	a family of communications security equipment
kHz	kilohertz
KIV-7	AlliedSignal embeddable KG-84 communications security module
LAN	local area network
LFP	live fly phase
LGSM	light ground station module
LSP	linked simulators phase
Mbps	megabits per second
MHz	megahertz
MIL-STD	military standard
MOA	memorandum of agreement
modem	modulator/demodulator
MRC	monthly recurring charges
ms	millisecond
NAS	naval air station
NAWC-WPNS	Naval Air Warfare Center Weapons Division
NetVisualizer™	software that displays real-time bandwidth use in a rolling bar graph format for quick visual reference
NIU	network interface unit
NRC	nonrecurring charges
NRNet	Near-Real-Time Network
NRZ	non-return to zero
NSA	National Security Agency
OT&E	operational test and evaluation
PCM	pulse code modulation
PDU	protocol data unit
PX	packet exchange
QAVP	quad-analog voice processor
RAD	the company that manufactures the voice signal converter
SGI	Silicon Graphics, Inc.
SIMLAB	Simulation Laboratory at the Naval Air Warfare Center, China Lake, California
SIPERNET	Secret Internet Protocol Router Network
SIT	System Integration Test
SNMP	Simple Network Management Protocol
SPECTRUM®	an instrumentation suite used to measure bandwidth utilization

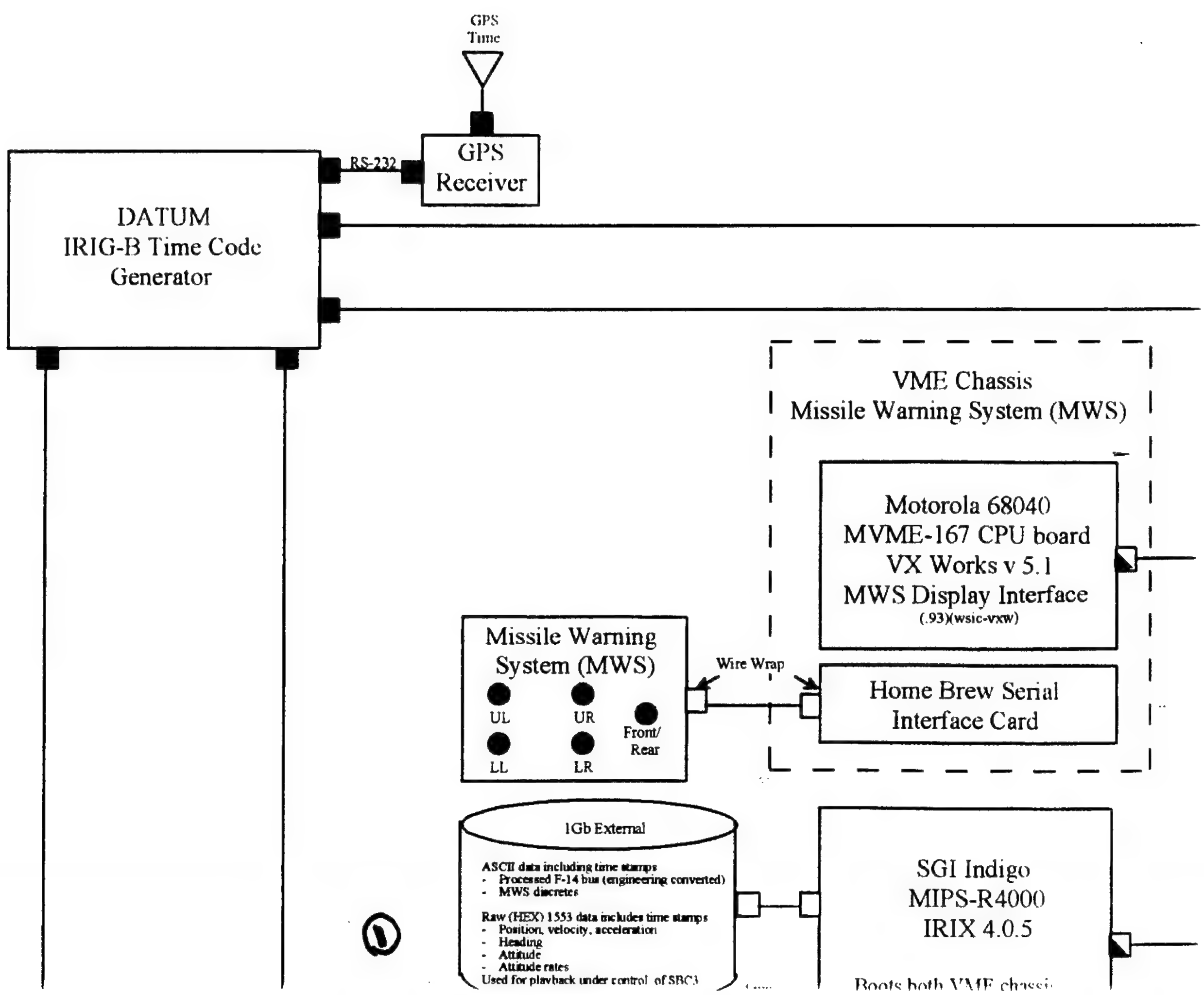
T&E	test and evaluation
T-1	digital carrier used to transmit a formatted digital signal at 1.544 megabits per second
T-3	28 T-1 lines in one; the aggregate data rate is 44.746 megabits per second
TCAC	Test Control and Analysis Center at JADS, Albuquerque, New Mexico
TCP	transmission control protocol
TDS	Timing Distribution System
UDP	user datagram protocol
V&V	verification and validation
VSC	voice signal converter
WAN	wide area network
WSIC	Weapons System Integration Center at Naval Air Warfare Center, Point Mugu, California
WSMR	White Sands Missile Range, New Mexico
WSSF	Weapon System Support Facility, China Lake, California
Y2K	year 2000

Appendix A

JADS Network Diagrams

Point Mugu , CA

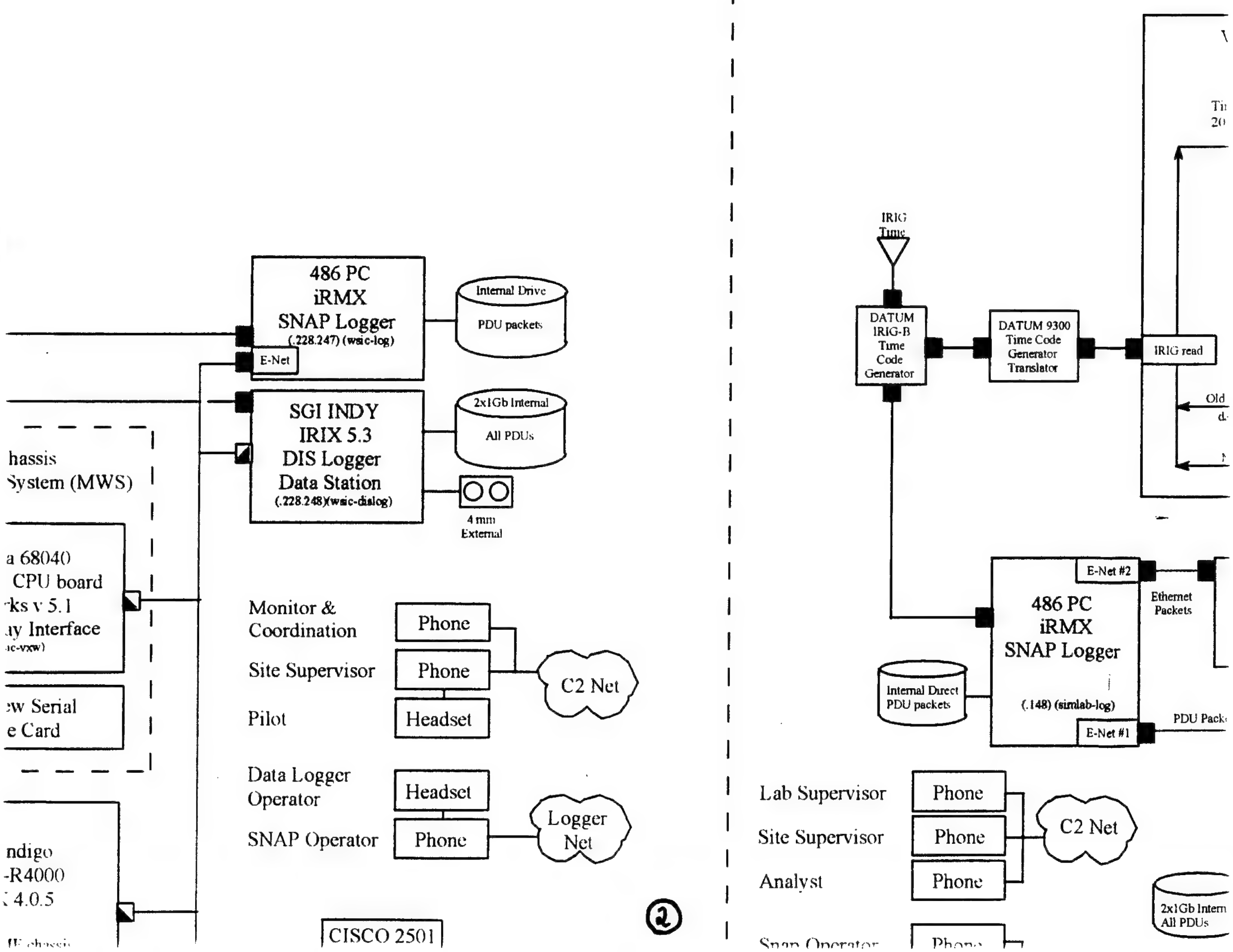
F-



Syst

gu , CA

F-14 Weapons System Integration Center (WSIC)
Room 300, Building 761
(Brian Krinsley)
(192.68.204.xxx)
(Subnet Broadcast: .255)



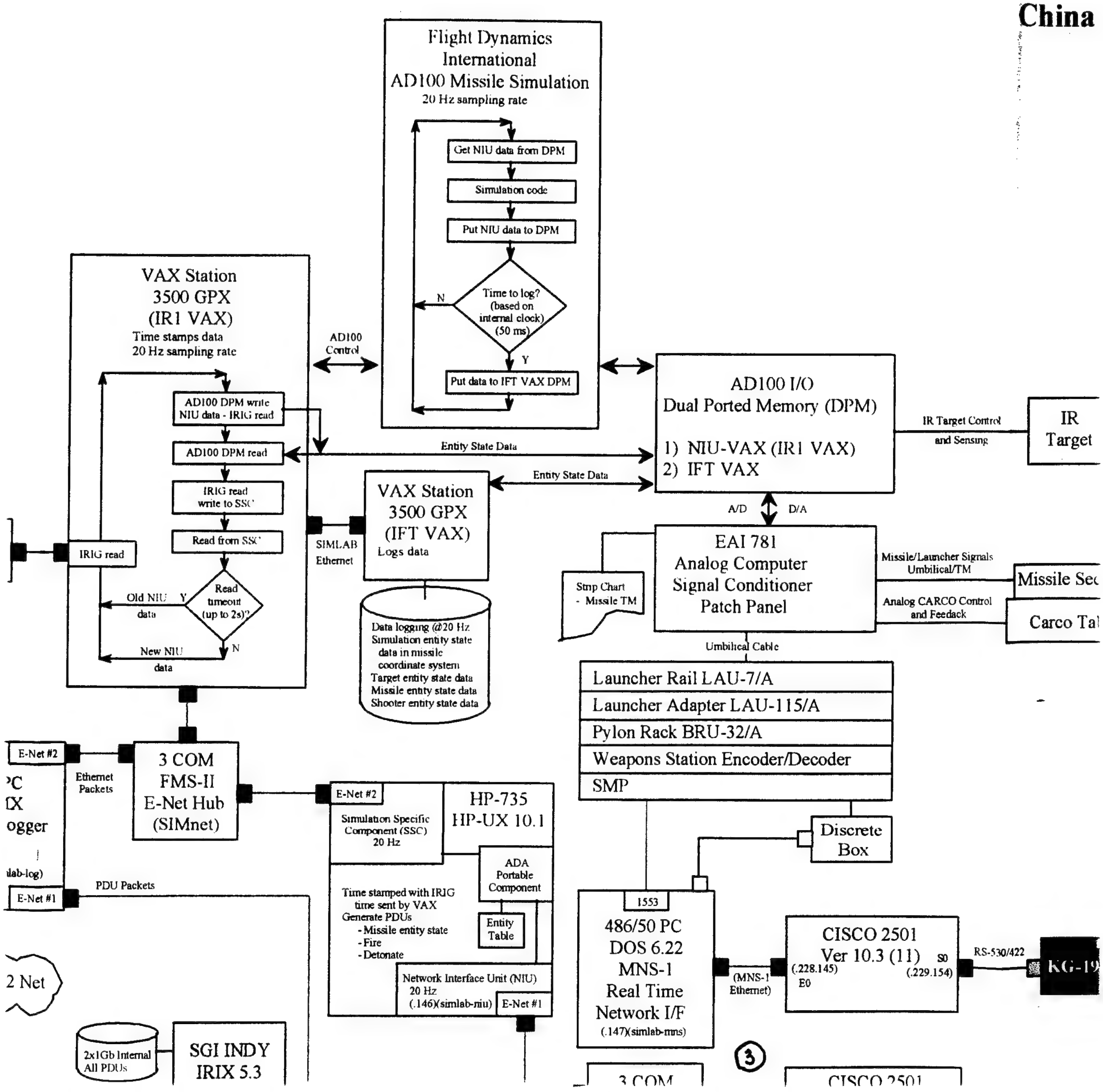
②

System Integration Test (SIT) Linked Simulators Phase (LSP)

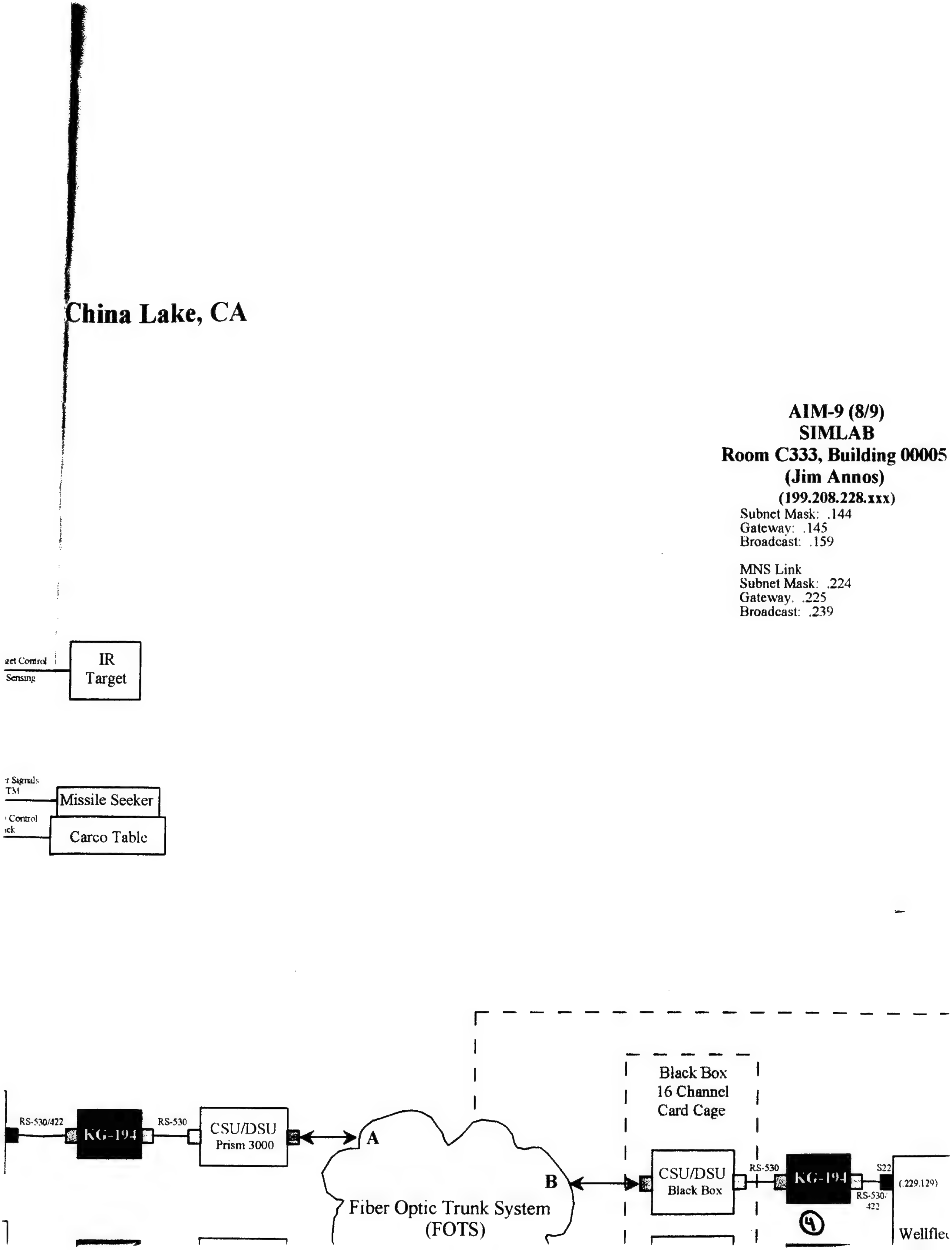
4/2 /97

Addresses:		Subnet Masks:
Host (Ethernet):	199.208.228.xxx	255.255.255.240
Serial (Router-to-router):	199.208.229.xxx	255.255.255.248

China



③

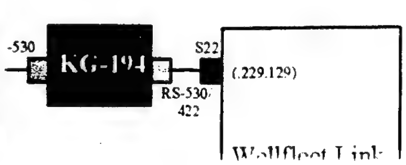

China Lake, CA
AIM-9 (8/9)
SIMLAB
Room C333, Building 00005
(Jim Annos)
(199.208.228.xxx)
Subnet Mask: .144
Gateway: .145
Broadcast: .159
MNS Link
Subnet Mask: .224
Gateway. .225
Broadcast: .239
IR Target
Missile Seeker
Carco Table
RS-530/422
KG-194
RS-530
CSU/DSU
Prism 3000
A
B
Fiber Optic Trunk System
(FOTS)
Black Box
16 Channel
Card Cage
CSU/DSU
Black Box
RS-530
KG-194
S22
(.229.129)
9

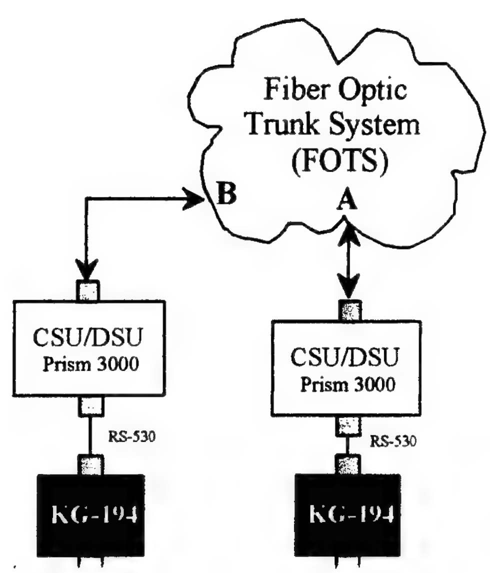
AIM-9 (8/9)
SIMLAB
ı C333, Building 00005
(Jim Annos)
(199.208.228.xxx)
net Mask: .144
:way: .145
ıdcast: .159

S Link
net Mask: .224
:way: .225
ıdcast: .239

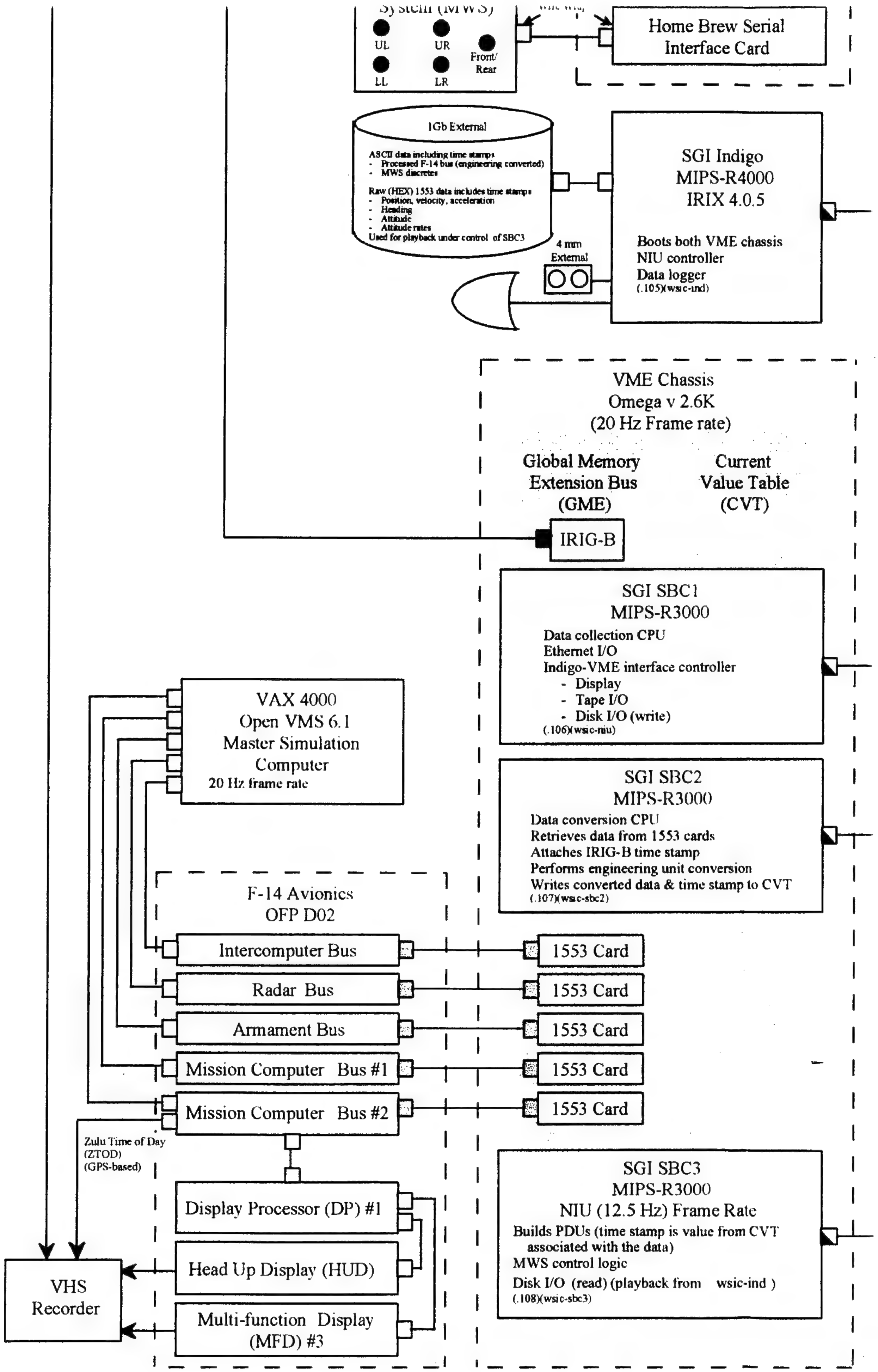
F/A-18 Weapon System Support Facility (WSSF)
Lab Room 115B, Building 20279
(Mike Campbell, Steve Zissos)
(199.208.228.xxx)
Subnet Mask: .192
Gateway: .193
Broadcast: .207

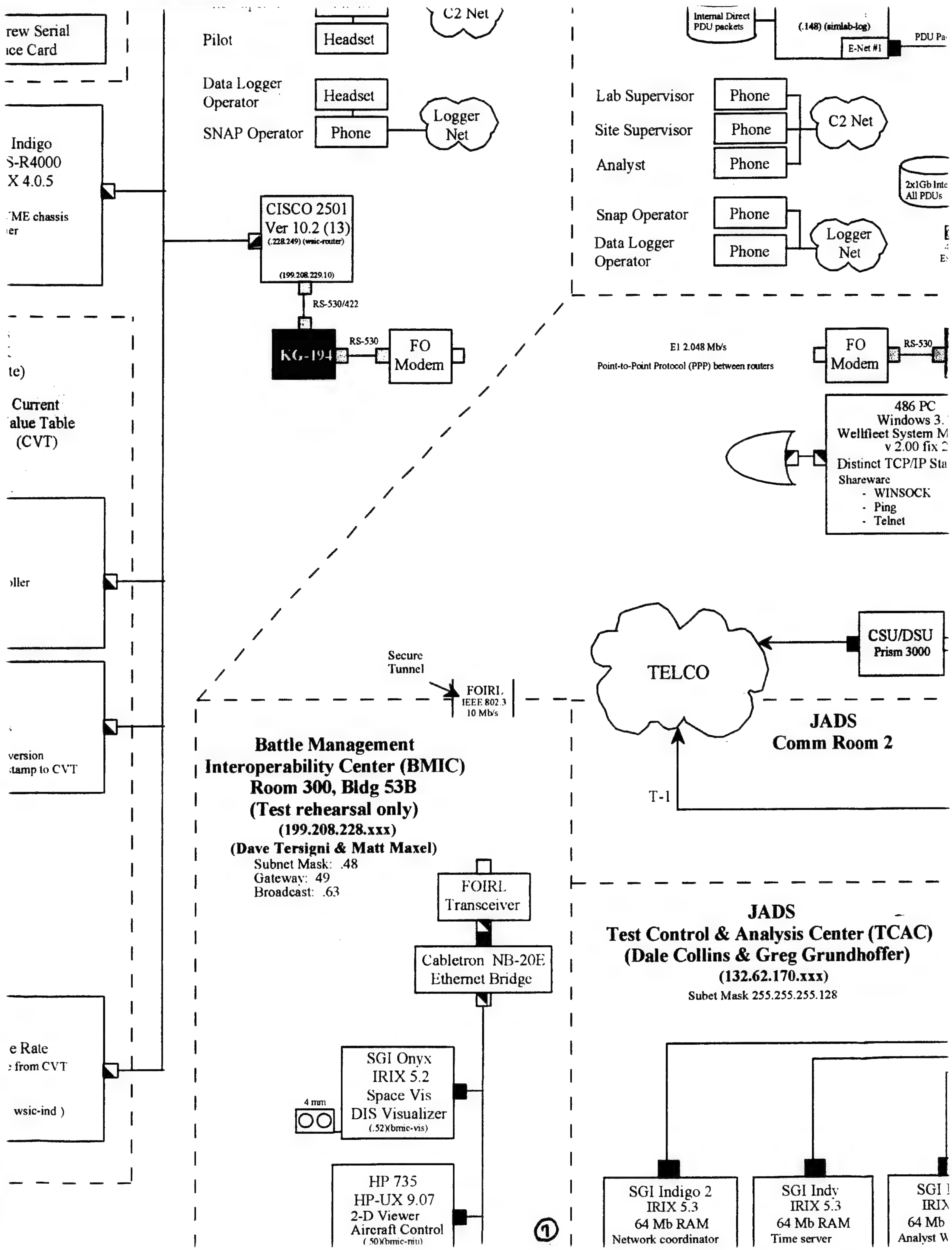
MNS Link
Subnet Mask: .208
Gateway: .209
Broadcast: .223



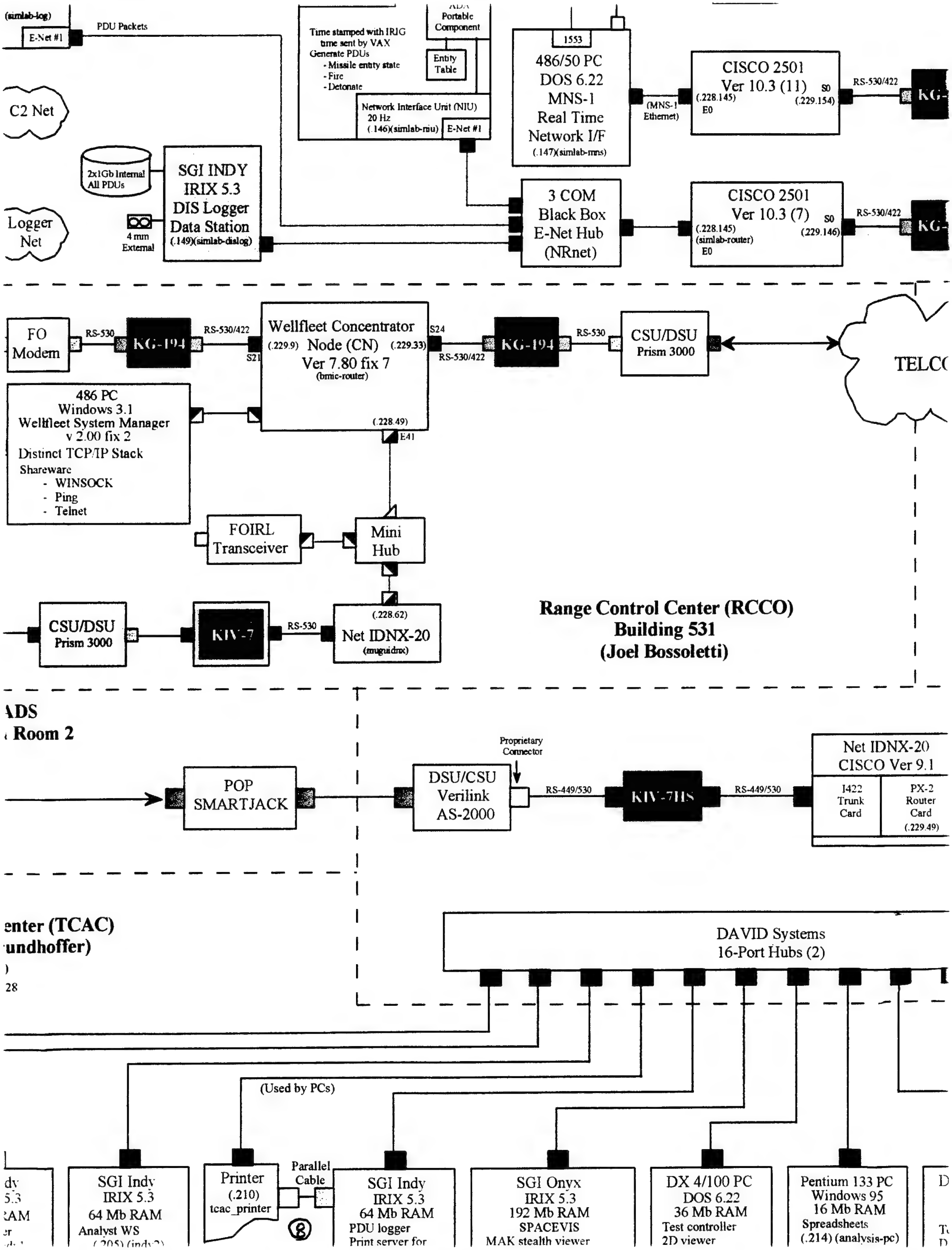


5

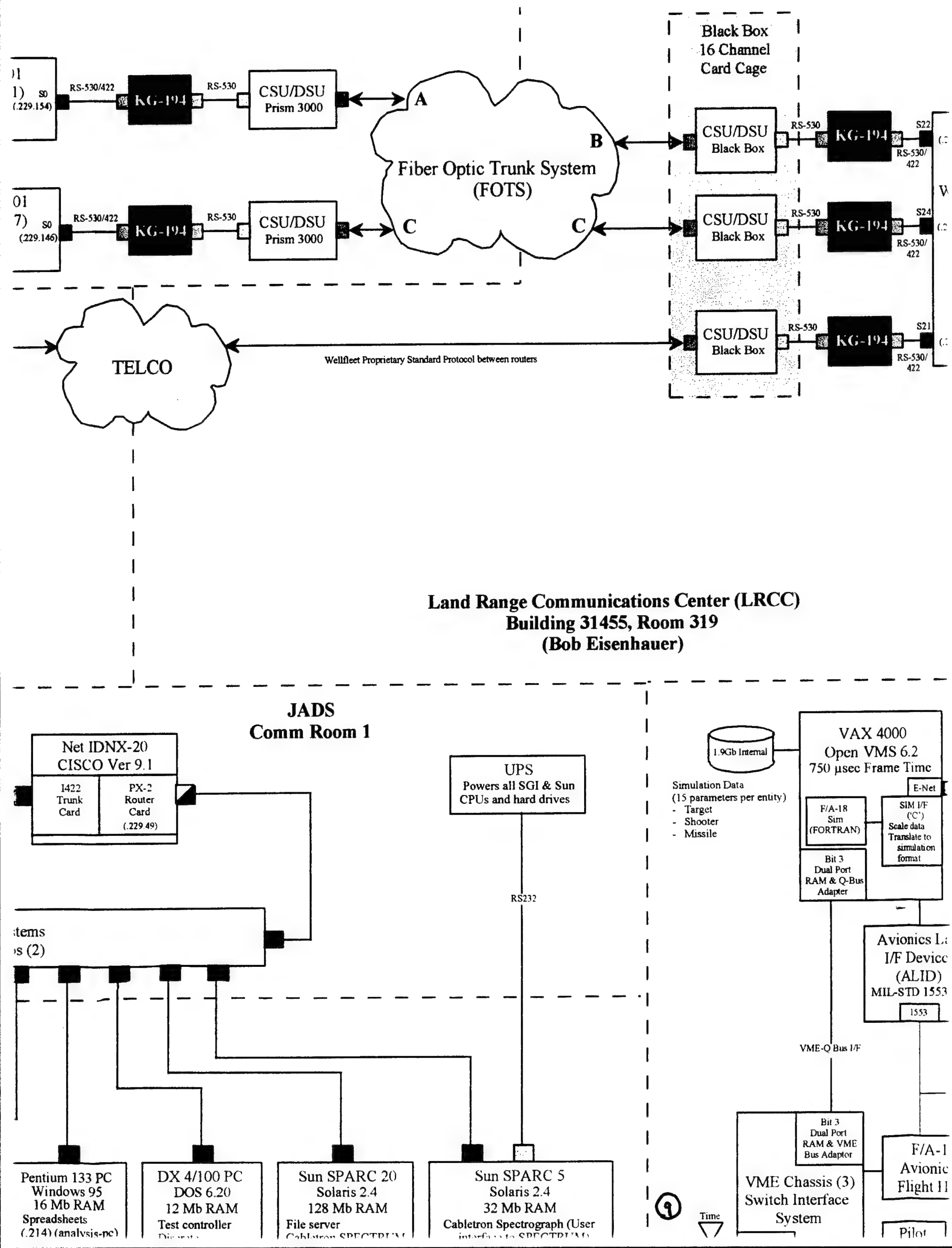

UL
UR
LL
LR
Front/ Rear
Home Brew Serial Interface Card
1Gb External
ASCII data including time stamps
- Processed F-14 bus (engineering converted)
- MWS discretes
Raw (HEX) 1553 data includes time stamps
- Position, velocity, acceleration
- Heading
- Attitude
- Attitude rates
Used for playback under control of SBC3
4 mm External
SGI Indigo
MIPS-R4000
IRIX 4.0.5
Boots both VME chassis
NIU controller
Data logger
(.105)(wsic-ind)
VME Chassis
Omega v 2.6K
(20 Hz Frame rate)
Global Memory Extension Bus (GME)
Current Value Table (CVT)
IRIG-B
SGI SBC1
MIPS-R3000
Data collection CPU
Ethernet I/O
Indigo-VME interface controller
- Display
- Tape I/O
- Disk I/O (write)
(.106)(wsic-niu)
VAX 4000
Open VMS 6.1
Master Simulation Computer
20 Hz frame rate
SGI SBC2
MIPS-R3000
Data conversion CPU
Retrieves data from 1553 cards
Attaches IRIG-B time stamp
Performs engineering unit conversion
Writes converted data & time stamp to CVT
(.107)(wsic-sbc2)
F-14 Avionics
OFP D02
Intercomputer Bus
Radar Bus
Armament Bus
Mission Computer Bus #1
Mission Computer Bus #2
1553 Card
1553 Card
1553 Card
1553 Card
1553 Card
Zulu Time of Day (ZTOD) (GPS-based)
Display Processor (DP) #1
Head Up Display (HUD)
Multi-function Display (MFD) #3
VHS Recorder
SGI SBC3
MIPS-R3000
NIU (12.5 Hz) Frame Rate
Builds PDUs (time stamp is value from CVT associated with the data)
MWS control logic
Disk I/O (read) (playback from wsic-ind)
(.108)(wsic-sbc3)



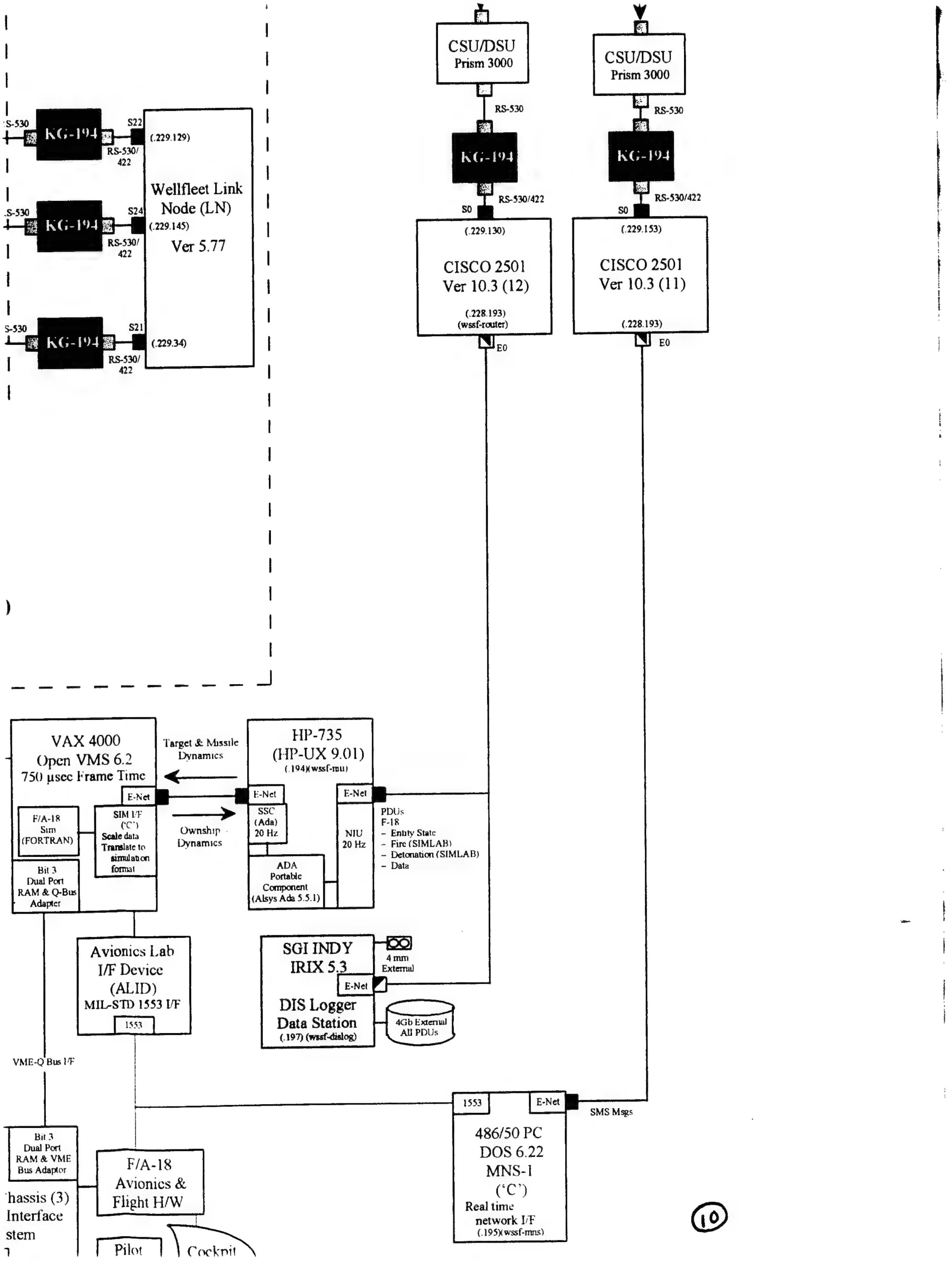
rew Serial
ice Card
Indigo
S-R4000
X 4.0.5
ME chassis
te)
Current
alue Table
(CVT)
version
tamp to CVT
e Rate
from CVT
wsic-ind)
Pilot
Headset
C2 Net
Data Logger
Operator
Headset
SNAP Operator
Phone
Logger
Net
CISCO 2501
Ver 10.2 (13)
(.228.249) (wsic-router)
(199.208.229.10)
RS-530/422
KG-194
RS-530
FO
Modem
Internal Direct
PDU packets
(.148) (simlab-log)
E-Net #1
PDU Pa
Lab Supervisor
Phone
Site Supervisor
Phone
C2 Net
Analyst
Phone
2x1Gb Inte
All PDUs
Snap Operator
Phone
Data Logger
Operator
Phone
Logger
Net
E1 2.048 Mb/s
Point-to-Point Protocol (PPP) between routers
FO
Modem
RS-530
486 PC
Windows 3.
Wellfleet System M
v 2.00 fix 2
Distinct TCP/IP Sta
Shareware
- WINSOCK
- Ping
- Telnet
TELCO
CSU/DSU
Prism 3000
Secure
Tunnel
FOIRL
IEEE 802.3
10 Mb/s
JADS
Comm Room 2
T-1
Battle Management
Interoperability Center (BMIC)
Room 300, Bldg 53B
(Test rehearsal only)
(199.208.228.xxx)
(Dave Tersigni & Matt Maxel)
Subnet Mask: .48
Gateway: 49
Broadcast: .63
FOIRL
Transceiver
Cabletron NB-20E
Ethernet Bridge
4 mm
SGI Onyx
IRIX 5.2
Space Vis
DIS Visualizer
(.52)(bmic-vis)
HP 735
HP-UX 9.07
2-D Viewer
Aircraft Control
(.50)(bmic-ntu)
1
JADS
Test Control & Analysis Center (TCAC)
(Dale Collins & Greg Grundhoffer)
(132.62.170.xxx)
Subet Mask 255.255.255.128
SGI Indigo 2
IRIX 5.3
64 Mb RAM
Network coordinator
SGI Indy
IRIX 5.3
64 Mb RAM
Time server
SGI I
IRIX
64 Mb
Analyst W



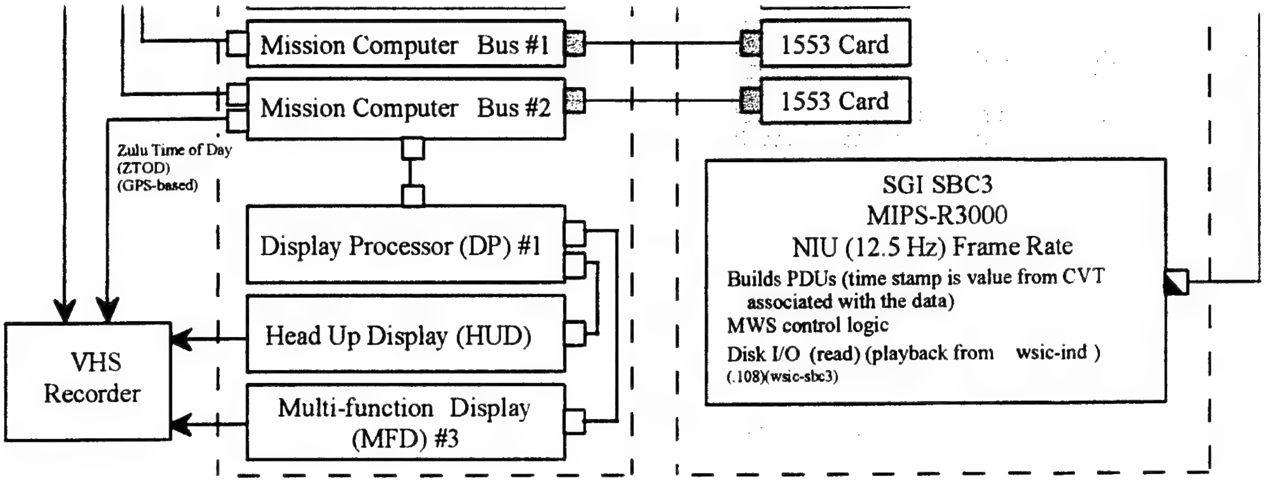
(simlab-log)
E-Net #1
PDU Packets
Time stamped with IRIG time sent by VAX
Generate PDUs
- Missile entity state
- Fire
- Detonate
Portable Component
Entity Table
Network Interface Unit (NIU)
20 Hz
(.146)(simlab-niu)
E-Net #1
1553
486/50 PC
DOS 6.22
MNS-1
Real Time
Network I/F
(.147)(simlab-mns)
(MNS-1 Ethernet)
CISCO 2501
Ver 10.3 (11)
(.228.145)
E0
S0
(.229.154)
RS-530/422
C2 Net
2x1Gb Internal
All PDUs
4 mm External
SGI INDY
IRIX 5.3
DIS Logger
Data Station
(.149)(simlab-dislog)
Logger Net
3 COM
Black Box
E-Net Hub
(NRnet)
CISCO 2501
Ver 10.3 (7)
(.228.145)
(simlab-router)
E0
S0
(229.146)
RS-530/422
FO Modem
RS-530
KG-194
RS-530/422
Wellfleet Concentrator
Node (CN)
(.229.9)
(.229.33)
S21
S24
Ver 7.80 fix 7
(bmic-router)
(.228.49)
E41
RS-530/422
KG-194
RS-530
CSU/DSU
Prism 3000
TELCO
486 PC
Windows 3.1
Wellfleet System Manager
v 2.00 fix 2
Distinct TCP/IP Stack
Shareware
- WINSOCK
- Ping
- Telnet
FOIRL Transceiver
Mini Hub
CSU/DSU
Prism 3000
KIV-7
RS-530
(.228.62)
Net IDNX-20
(muguidnx)
Range Control Center (RCCO)
Building 531
(Joel Bossoletti)
ADS
Room 2
POP SMARTJACK
Proprietary Connector
DSU/CSU
Verilink
AS-2000
RS-449/530
KIV-7HS
RS-449/530
Net IDNX-20
CISCO Ver 9.1
I422 Trunk Card
PX-2 Router Card
(.229.49)
enter (TCAC)
undhoffer)
28
DAVID Systems
16-Port Hubs (2)
(Used by PCs)
SGI Indy
IRIX 5.3
64 Mb RAM
Analyst WS
Printer
(.210)
tcac_printer
Parallel Cable
SGI Indy
IRIX 5.3
64 Mb RAM
PDU logger
Print server for
SGI Onyx
IRIX 5.3
192 Mb RAM
SPACEVIS
MAK stealth viewer
DX 4/100 PC
DOS 6.22
36 Mb RAM
Test controller
2D viewer
Pentium 133 PC
Windows 95
16 Mb RAM
Spreadsheets
(.214) (analysis-pc)
8

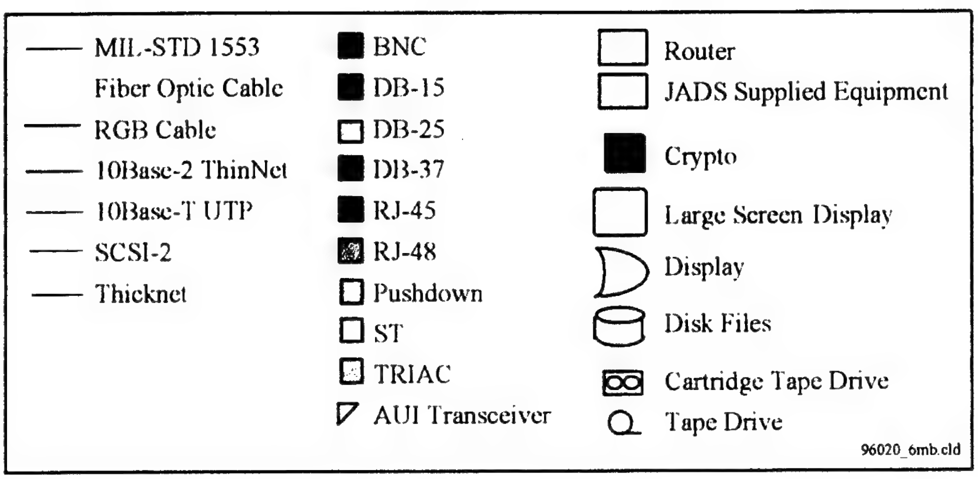


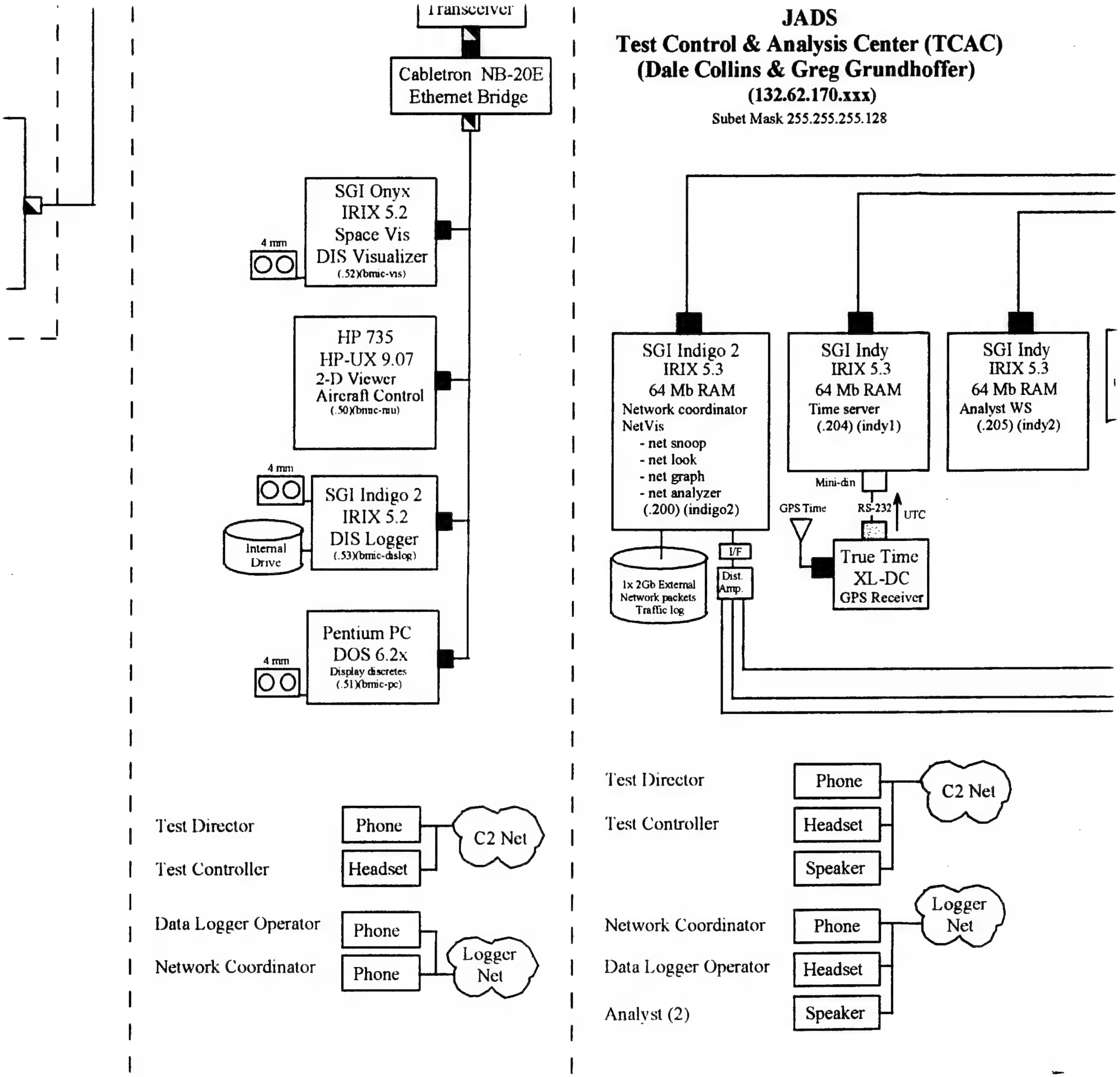
RS-530/422
KG-194
RS-530
CSU/DSU
Prism 3000
A
B
C
Fiber Optic Trunk System
(FOTS)
Black Box
16 Channel
Card Cage
CSU/DSU
Black Box
RS-530/
422
S22
S24
S21
S0
(.229.154)
(229.146)
TELCO
Wellfleet Proprietary Standard Protocol between routers
Land Range Communications Center (LRCC)
Building 31455, Room 319
(Bob Eisenhauer)
JADS
Comm Room 1
Net IDNX-20
CISCO Ver 9.1
1422
Trunk
Card
PX-2
Router
Card
(.229.49)
UPS
Powers all SGI & Sun
CPUs and hard drives
RS232
1.9Gb Internal
Simulation Data
(15 parameters per entity)
- Target
- Shooter
- Missile
VAX 4000
Open VMS 6.2
750 µsec Frame Time
E-Net
F/A-18
Sim
(FORTRAN)
SIM I/F
('C')
Scale data
Translate to
simulation
format
Bit 3
Dual Port
RAM & Q-Bus
Adapter
Avionics
I/F Device
(ALID)
MIL-STD 1553
1553
VME-Q Bus I/F
Bit 3
Dual Port
RAM & VME
Bus Adaptor
VME Chassis (3)
Switch Interface
System
F/A-1
Avionic
Flight
Pilot
Pentium 133 PC
Windows 95
16 Mb RAM
Spreadsheets
(.214) (analysis-pc)
DX 4/100 PC
DOS 6.20
12 Mb RAM
Test controller
Sun SPARC 20
Solaris 2.4
128 Mb RAM
File server
Sun SPARC 5
Solaris 2.4
32 Mb RAM
Cabletron Spectrograph (User
Time
9

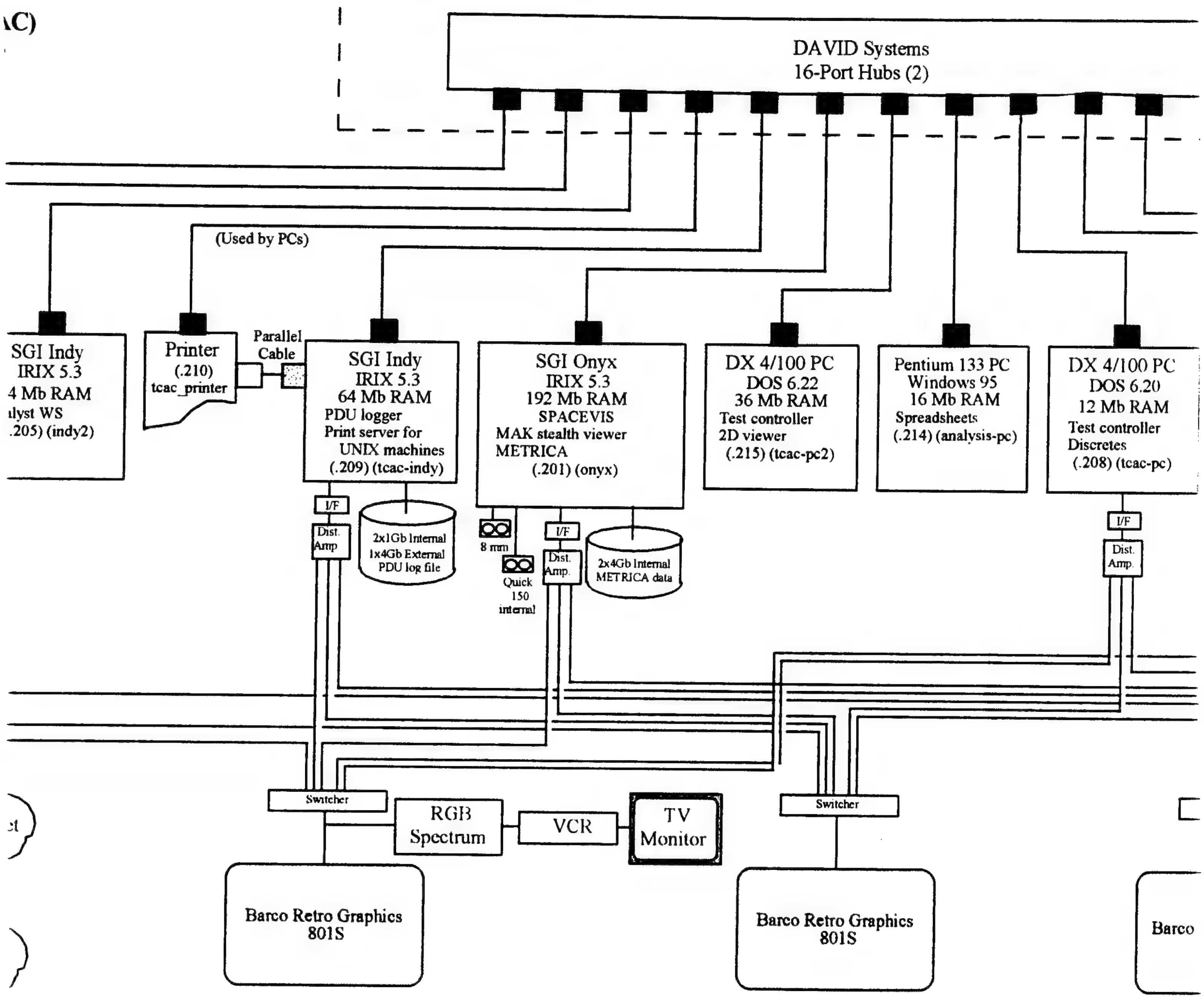


S-530
KG-194
S22
(.229.129)
RS-530/422
Wellfleet Link Node (LN)
Ver 5.77
S-530
KG-194
S24
(.229.145)
RS-530/422
S-530
KG-194
S21
(.229.34)
RS-530/422
CSU/DSU
Prism 3000
RS-530
KG-194
RS-530/422
S0
(.229.130)
CISCO 2501
Ver 10.3 (12)
(.228.193)
(wssf-router)
E0
CSU/DSU
Prism 3000
RS-530
KG-194
RS-530/422
S0
(.229.153)
CISCO 2501
Ver 10.3 (11)
(.228.193)
E0
VAX 4000
Open VMS 6.2
750 µsec Frame Time
E-Net
F/A-18
Sim
(FORTRAN)
SIM I/F
('C')
Scale data
Translate to simulation format
Bit 3
Dual Port
RAM & Q-Bus
Adapter
Target & Missile
Dynamics
Ownship
Dynamics
HP-735
(HP-UX 9.01)
(.194)(wssf-mu)
E-Net
SSC
(Ada)
20 Hz
E-Net
NIU
20 Hz
ADA
Portable
Component
(Alsys Ada 5.5.1)
PDUs
F-18
- Entity State
- Fire (SIMLAB)
- Detonation (SIMLAB)
- Data
Avionics Lab
I/F Device
(ALID)
MIL-STD 1553 I/F
1553
SGI INDY
IRIX 5.3
E-Net
DIS Logger
Data Station
(.197) (wssf-dislog)
4 mm
External
4Gb External
All PDUs
VME-Q Bus I/F
Bit 3
Dual Port
RAM & VME
Bus Adaptor
hassis (3)
Interface
stem
F/A-18
Avionics &
Flight H/W
Pilot
Cockpit
1553
E-Net
SMS Msgs
486/50 PC
DOS 6.22
MNS-1
('C')
Real time
network I/F
(.195)(wssf-mns)

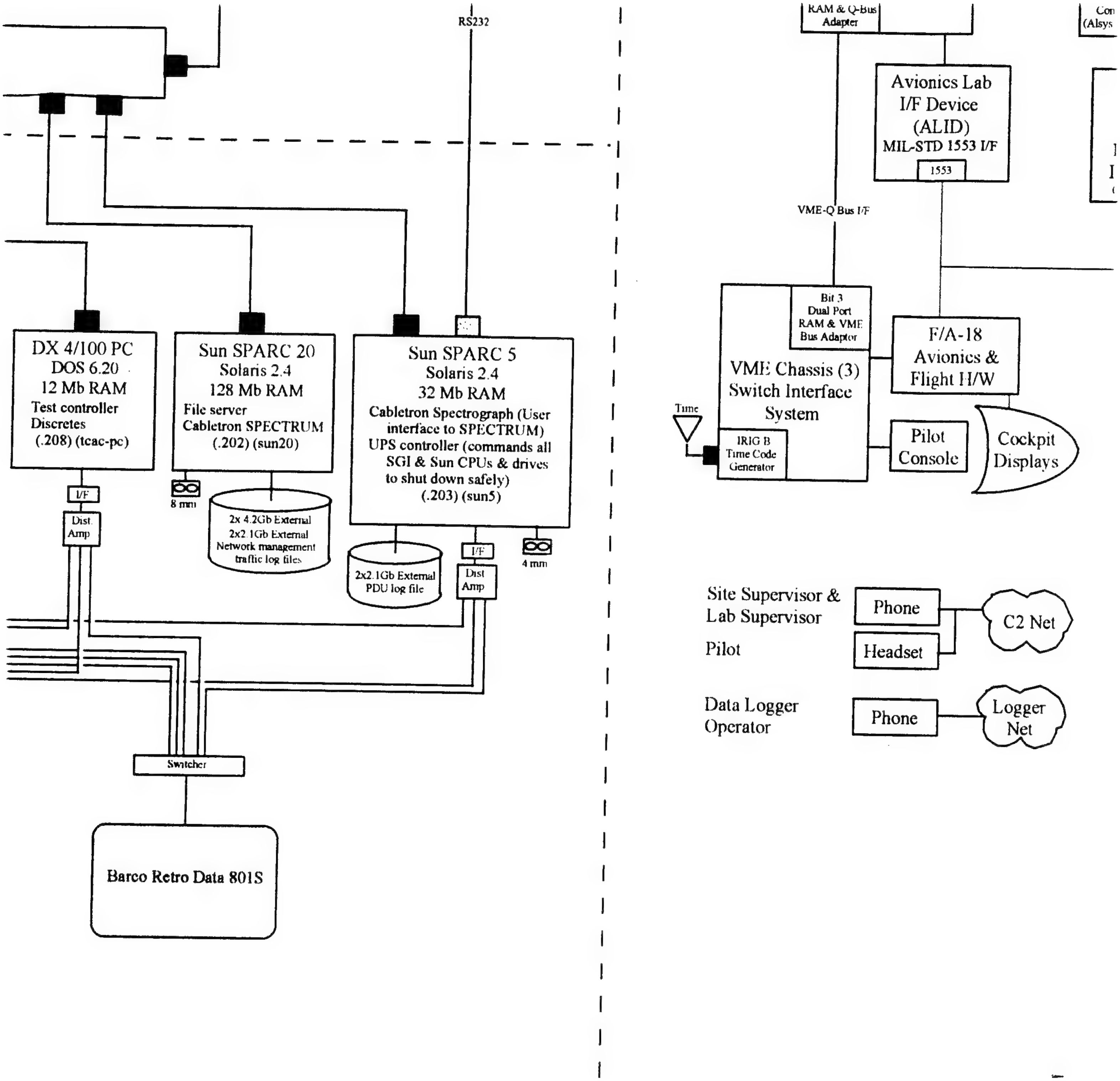

Mission Computer Bus #1
Mission Computer Bus #2
1553 Card
1553 Card
Zulu Time of Day (ZTOD) (GPS-based)
Display Processor (DP) #1
Head Up Display (HUD)
Multi-function Display (MFD) #3
VHS Recorder
SGI SBC3
MIPS-R3000
NIU (12.5 Hz) Frame Rate
Builds PDUs (time stamp is value from CVT associated with the data)
MWS control logic
Disk I/O (read) (playback from wsic-ind)
(.108)(wsic-sbc3)

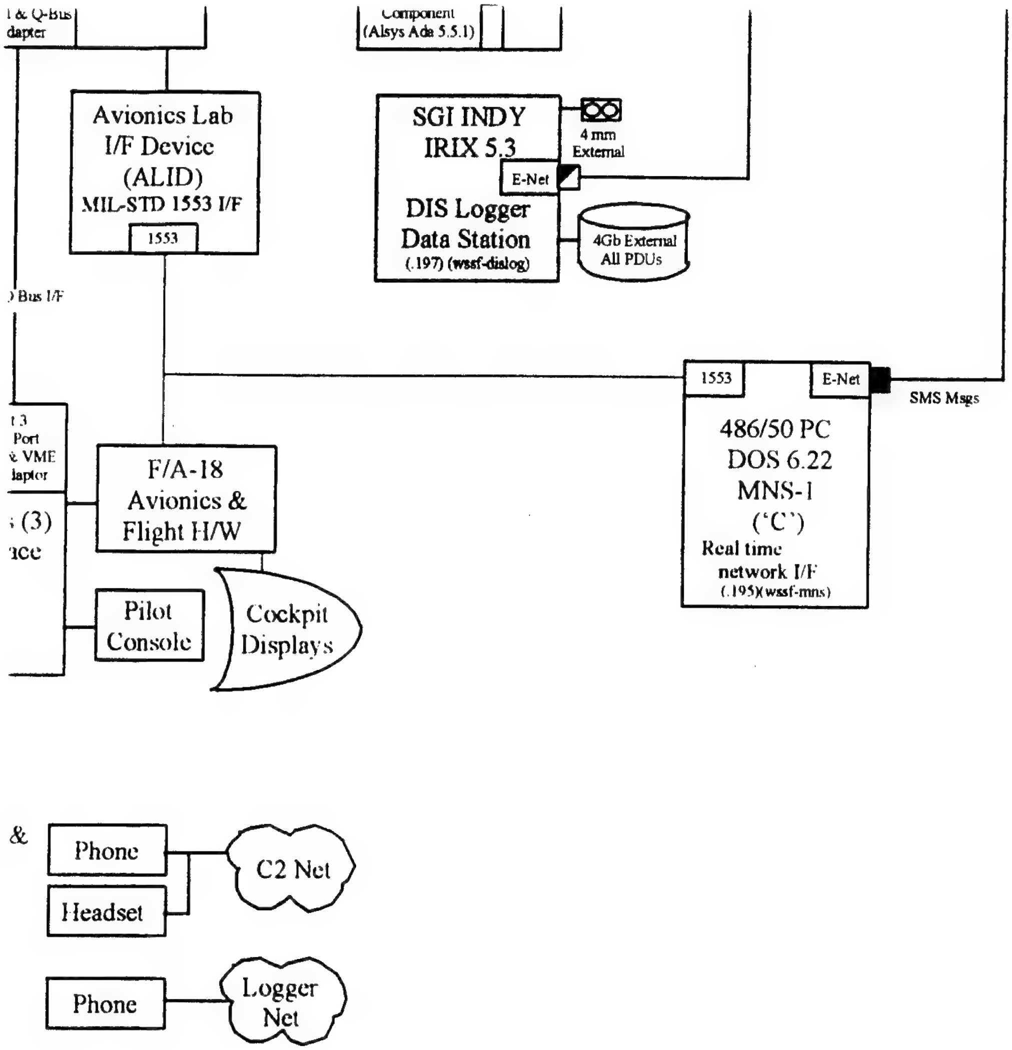

MIL-STD 1553
Fiber Optic Cable
RGB Cable
10Base-2 ThinNet
10Base-T UTP
SCSI-2
Thicknet
BNC
DB-15
DB-25
DB-37
RJ-45
RJ-48
Pushdown
ST
TRIAC
AUI Transceiver
Router
JADS Supplied Equipment
Crypto
Large Screen Display
Display
Disk Files
Cartridge Tape Drive
Tape Drive
96020_6mb.cld


Transceiver
Cabletron NB-20E Ethernet Bridge
SGI Onyx
IRIX 5.2
Space Vis
DIS Visualizer
(.52)(bmic-vis)
4 mm
HP 735
HP-UX 9.07
2-D Viewer
Aircraft Control
(.50)(bmic-mu)
4 mm
SGI Indigo 2
IRIX 5.2
DIS Logger
(.53)(bmic-dslog)
Internal Drive
Pentium PC
DOS 6.2x
Display discretes
(.51)(bmic-pc)
4 mm
Test Director
Test Controller
Phone
Headset
C2 Net
Data Logger Operator
Network Coordinator
Phone
Phone
Logger Net
JADS
Test Control & Analysis Center (TCAC)
(Dale Collins & Greg Grundhoffer)
(132.62.170.xxx)
Subet Mask 255.255.255.128
SGI Indigo 2
IRIX 5.3
64 Mb RAM
Network coordinator
NetVis
- net snoop
- net look
- net graph
- net analyzer
(.200) (indigo2)
SGI Indy
IRIX 5.3
64 Mb RAM
Time server
(.204) (indy1)
SGI Indy
IRIX 5.3
64 Mb RAM
Analyst WS
(.205) (indy2)
Mini-din
GPS Time
RS-232
UTC
True Time
XL-DC
GPS Receiver
I/F
Dist. Amp.
1x 2Gb External
Network packets
Traffic log
Test Director
Test Controller
Phone
Headset
Speaker
C2 Net
Network Coordinator
Data Logger Operator
Analyst (2)
Phone
Headset
Speaker
Logger Net

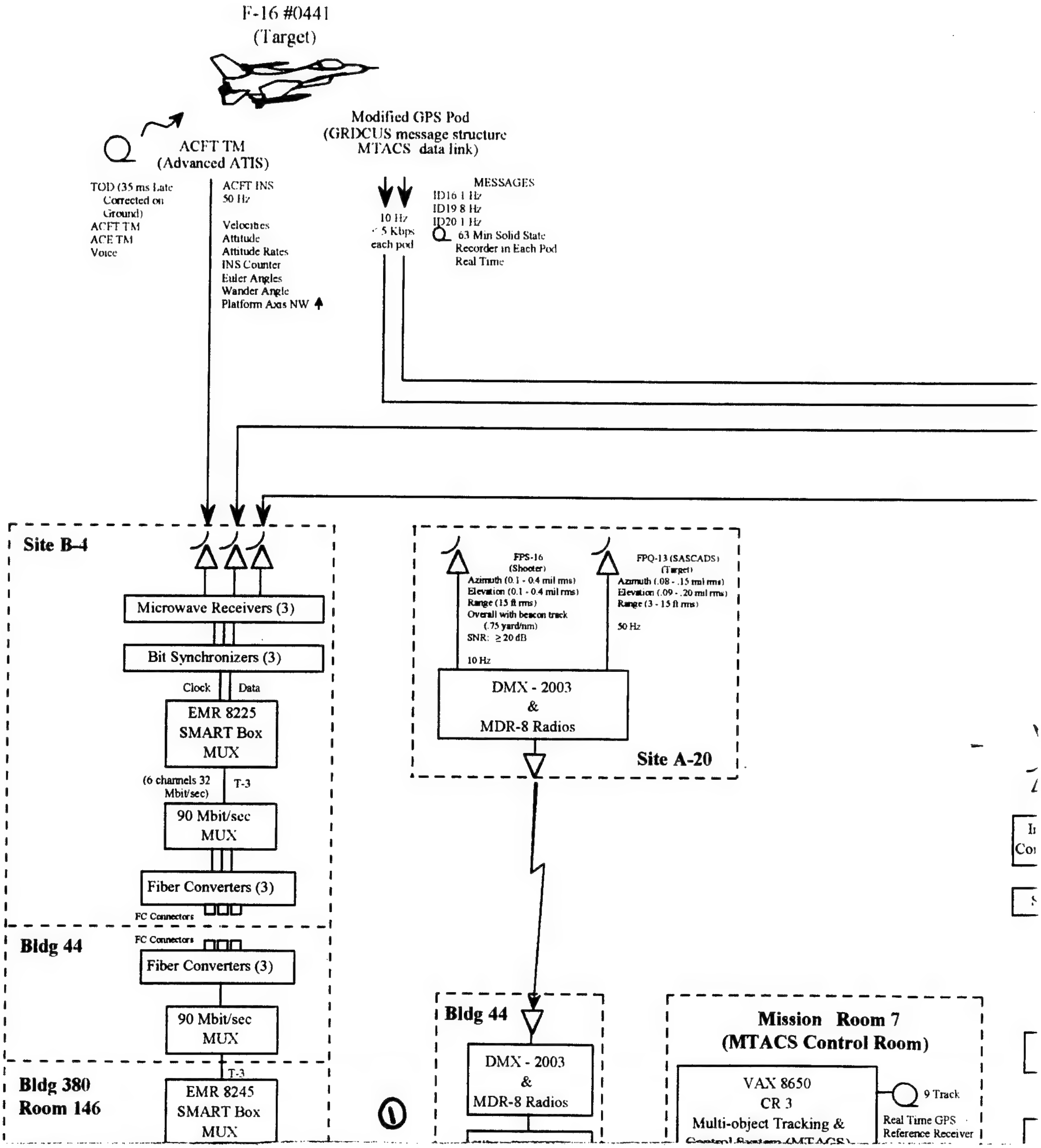


Albuquerque, NM
(Live Missions Only)


RS232
RAM & Q-Bus Adapter
Con (Alsys
Avionics Lab I/F Device (ALID)
MIL-STD 1553 I/F
1553
VME-Q Bus I/F
Bit 3 Dual Port RAM & VME Bus Adaptor
VME Chassis (3) Switch Interface System
IRIG B Time Code Generator
Time
F/A-18 Avionics & Flight H/W
Pilot Console
Cockpit Displays
DX 4/100 PC
DOS 6.20
12 Mb RAM
Test controller
Discretes
(.208) (tcac-pc)
Sun SPARC 20
Solaris 2.4
128 Mb RAM
File server
Cabletron SPECTRUM
(.202) (sun20)
Sun SPARC 5
Solaris 2.4
32 Mb RAM
Cabletron Spectrograph (User interface to SPECTRUM)
UPS controller (commands all SGI & Sun CPUs & drives to shut down safely)
(.203) (sun5)
I/F
Dist. Amp
8 mm
2x 4.2Gb External
2x2.1Gb External
Network management traffic log files
2x2.1Gb External
PDU log file
I/F
Dist Amp
4 mm
Site Supervisor & Lab Supervisor
Phone
C2 Net
Pilot
Headset
Data Logger Operator
Phone
Logger Net
Switcher
Barco Retro Data 801S

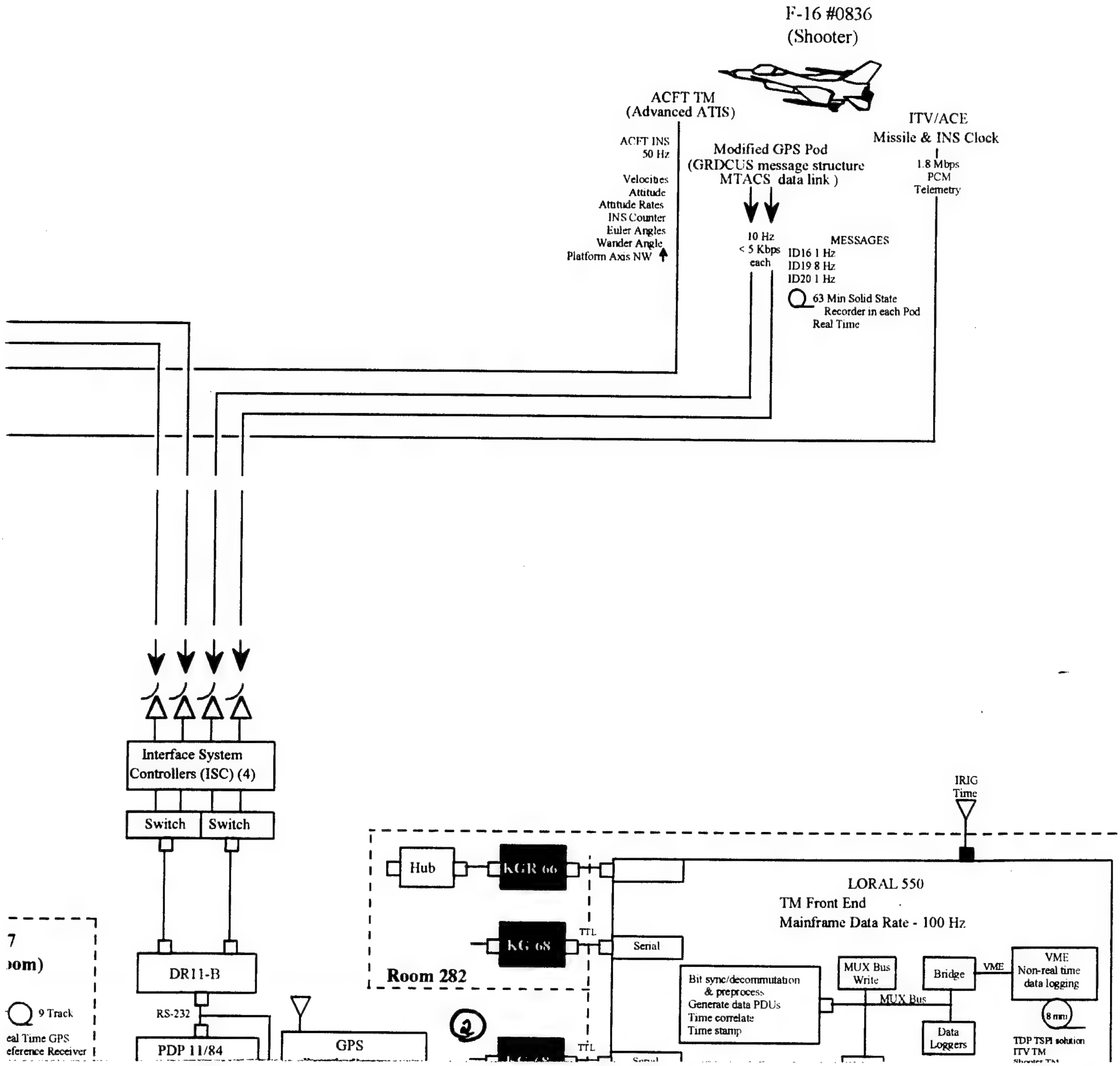


l & Q-Bus
dapter
Component
(Alsys Ada 5.5.1)
Avionics Lab
I/F Device
(ALID)
MIL-STD 1553 I/F
1553
SGI INDY
IRIX 5.3
E-Net
DIS Logger
Data Station
(.197) (wssf-dialog)
4 mm
External
4Gb External
All PDUs
) Bus I/F
1553
E-Net
SMS Msgs
486/50 PC
DOS 6.22
MNS-1
('C')
Real time
network I/F
(.195)(wssf-mns)
t 3
Port
& VME
dapter
F/A-18
Avionics &
Flight H/W
; (3)
ace
Pilot
Console
Cockpit
Displays
&
Phone
Headset
C2 Net
Phone
Logger
Net



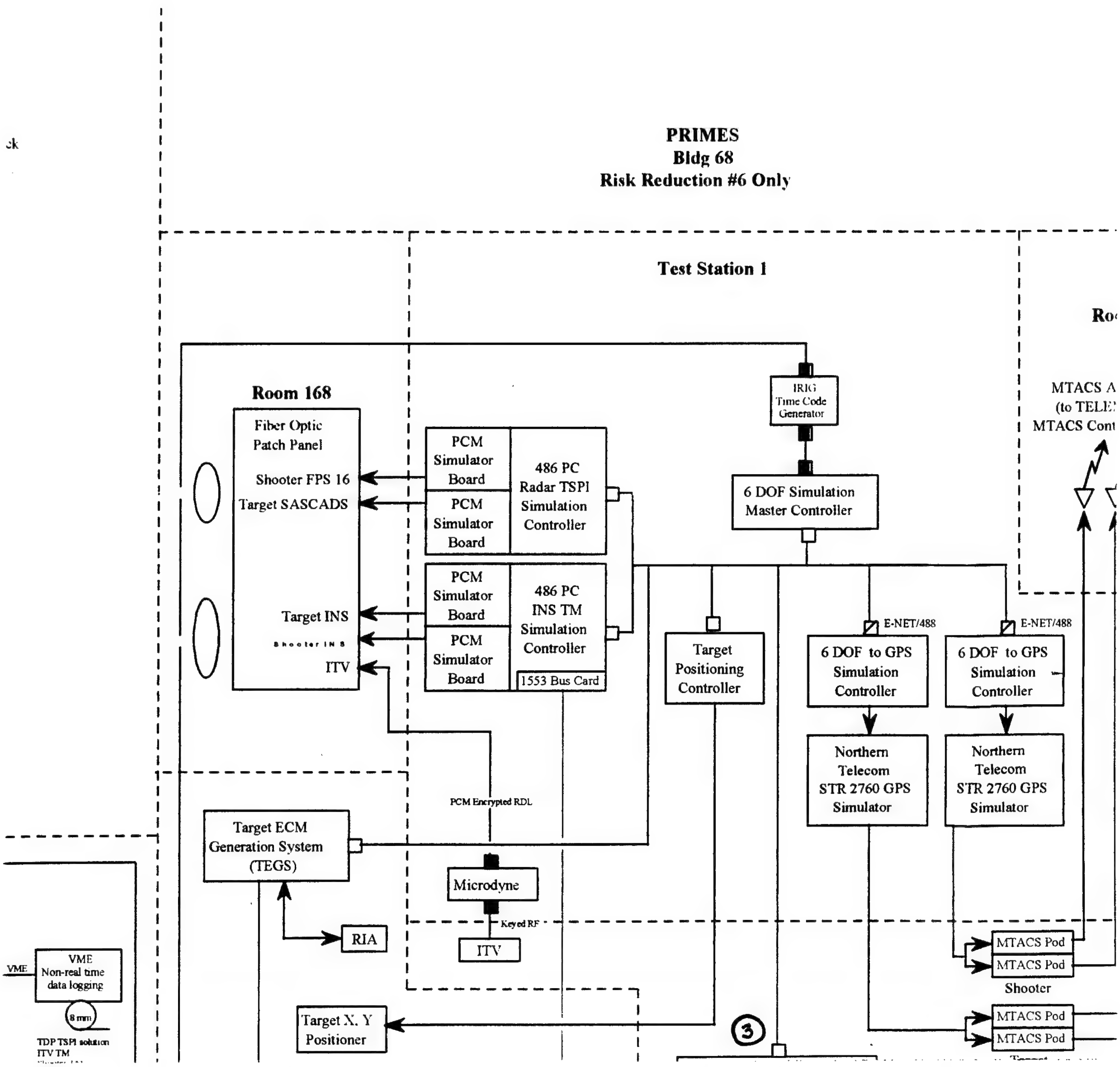
F-16 #0441
(Target)
ACFT TM
(Advanced ATIS)
TOD (35 ms Late Corrected on Ground)
ACFT TM
ACE TM
Voice
ACFT INS
50 Hz
Velocities
Attitude
Attitude Rates
INS Counter
Euler Angles
Wander Angle
Platform Axis NW
Modified GPS Pod
(GRIDCUS message structure
MTACS data link)
10 Hz
< 5 Kbps
each pod
MESSAGES
ID16 1 Hz
ID19 8 Hz
ID20 1 Hz
63 Min Solid State Recorder in Each Pod
Real Time
Site B-4
Microwave Receivers (3)
Bit Synchronizers (3)
Clock
Data
EMR 8225
SMART Box
MUX
(6 channels 32 Mbit/sec)
T-3
90 Mbit/sec
MUX
Fiber Converters (3)
FC Connectors
Bldg 44
FC Connectors
Fiber Converters (3)
90 Mbit/sec
MUX
Bldg 380
Room 146
T-3
EMR 8245
SMART Box
MUX
FPS-16
(Shooter)
Azimuth (0.1 - 0.4 mil rms)
Elevation (0.1 - 0.4 mil rms)
Range (15 ft rms)
Overall with beacon track
(.75 yard/nm)
SNR: ≥ 20 dB
10 Hz
FPQ-13 (SASCADS)
(Target)
Azimuth (.08 - .15 mil rms)
Elevation (.09 - .20 mil rms)
Range (3 - 15 ft rms)
50 Hz
DMX - 2003
&
MDR-8 Radios
Site A-20
Bldg 44
DMX - 2003
&
MDR-8 Radios
Mission Room 7
(MTACS Control Room)
VAX 8650
CR 3
Multi-object Tracking &
9 Track
Real Time GPS Reference Receiver

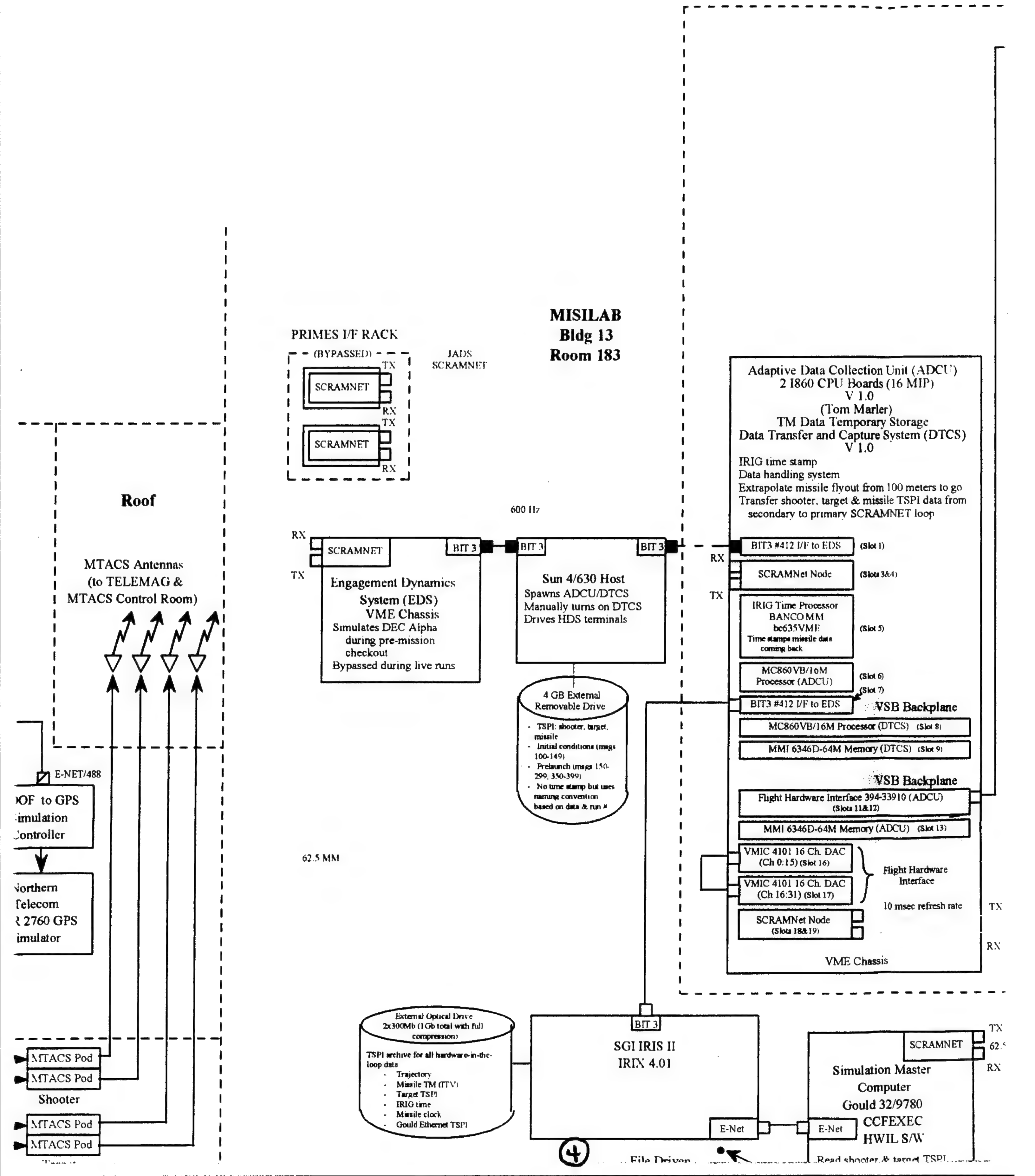
①

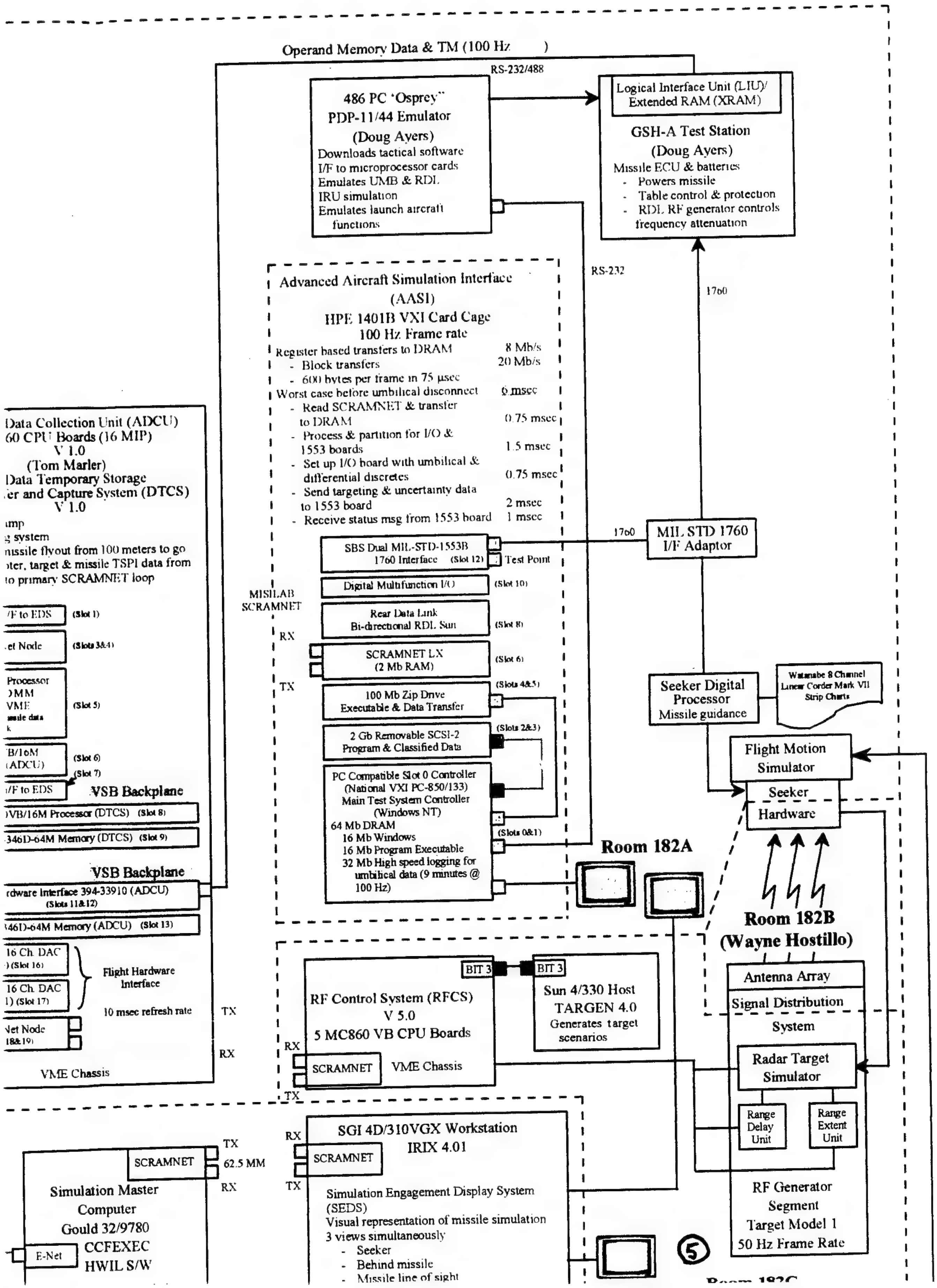


F-16 #0836
(Shooter)
ACFT TM
(Advanced ATIS)
ACFT INS
50 Hz
Velocities
Attitude
Attitude Rates
INS Counter
Euler Angles
Wander Angle
Platform Axis NW
Modified GPS Pod
(GRDCUS message structure
MTACS data link)
10 Hz
< 5 Kbps
each
MESSAGES
ID16 1 Hz
ID19 8 Hz
ID20 1 Hz
63 Min Solid State
Recorder in each Pod
Real Time
ITV/ACE
Missile & INS Clock
1.8 Mbps
PCM
Telemetry
Interface System
Controllers (ISC) (4)
Switch
Switch
DR11-B
RS-232
PDP 11/84
GPS
9 Track
eal Time GPS
eference Receiver
7
oom)
IRIG
Time
Hub
KGR 66
KG 68
TTL
Serial
Room 282
LORAL 550
TM Front End
Mainframe Data Rate - 100 Hz
Bit sync/decommutation
& preprocess
Generate data PDUs
Time correlate
Time stamp
MUX Bus
Write
MUX Bus
Bridge
VME
VME
Non-real time
data logging
8 mm
Data
Loggers
TDP TSPI solution
ITV TM

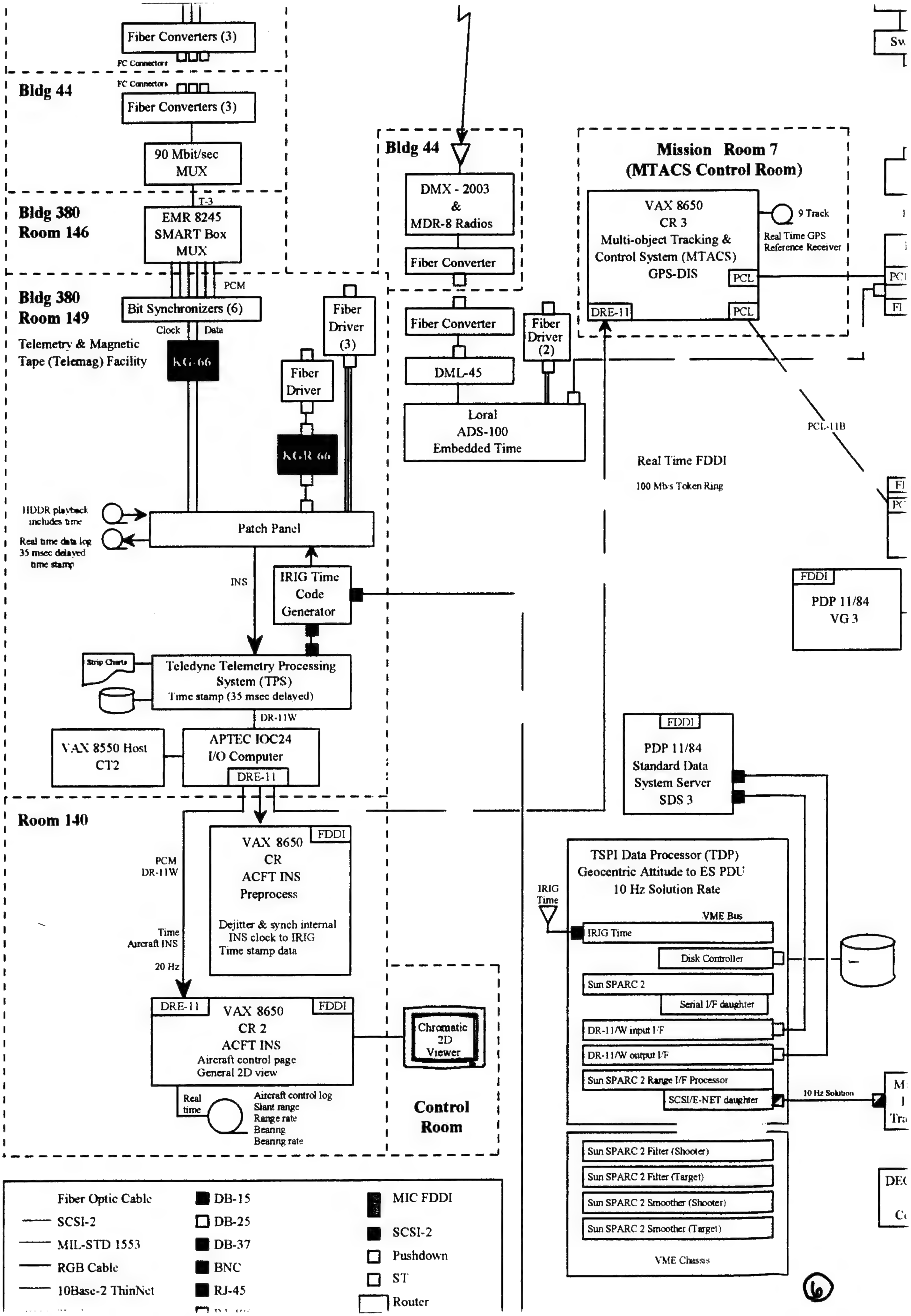
System Integration Test (Live Fly Phase)
Eglin AFB, FL

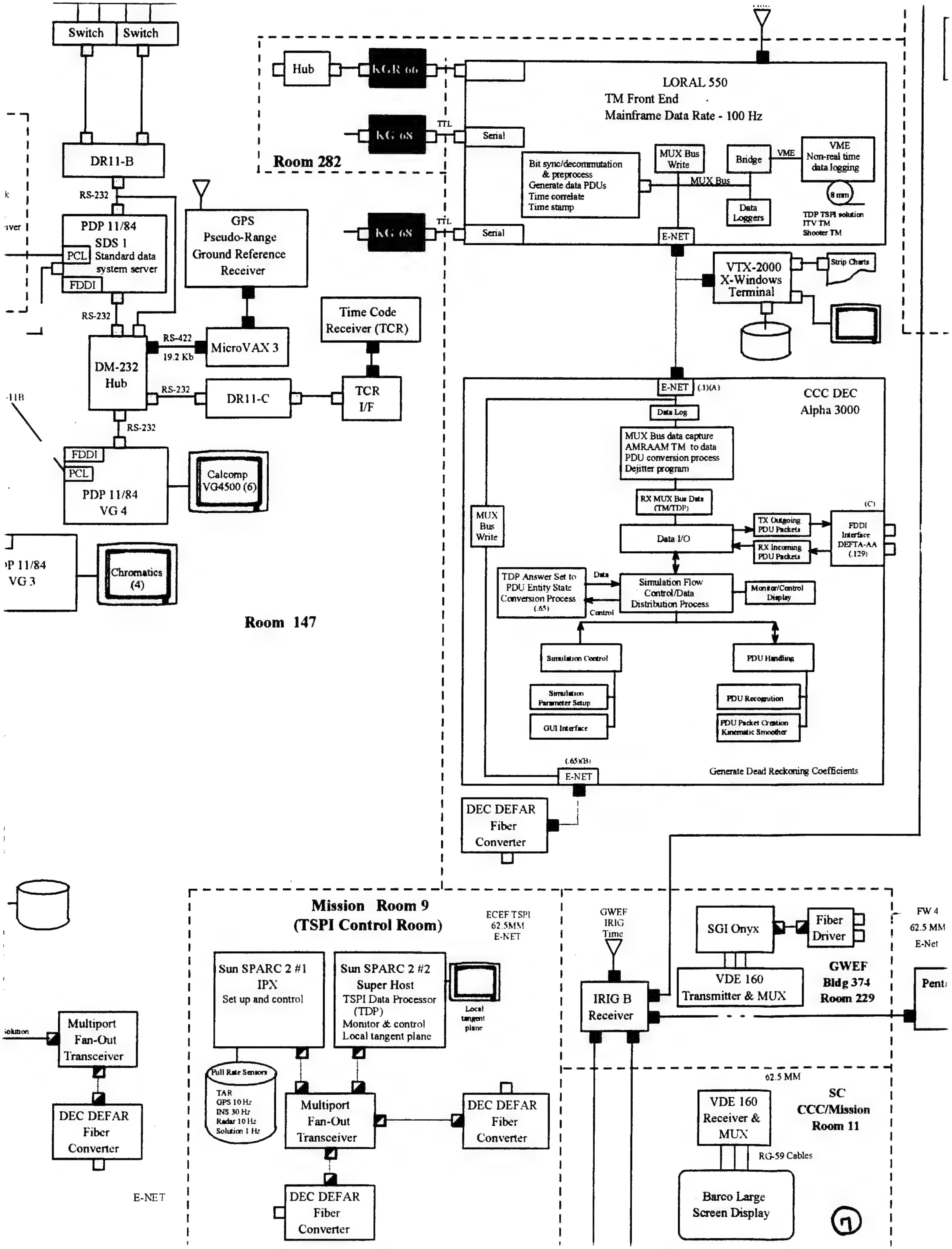



MISILAB
Bldg 13
Room 183
PRIMES I/F RACK
(BYPASSED)
SCRAMNET
SCRAMNET
TX
RX
JADS SCRAMNET
Roof
MTACS Antennas
(to TELEMAG &
MTACS Control Room)
600 Hz
SCRAMNET
BIT 3
Engagement Dynamics System (EDS)
VME Chassis
Simulates DEC Alpha during pre-mission checkout
Bypassed during live runs
Sun 4/630 Host
Spawns ADCU/DTCS
Manually turns on DTCS
Drives HDS terminals
4 GB External Removable Drive
TSPI: shooter, target, missile
Initial conditions (msgs 100-149)
Prelaunch (msgs 150-299, 350-399)
No time stamp but uses naming convention based on data & run #
Adaptive Data Collection Unit (ADCU)
2 I860 CPU Boards (16 MIP)
V 1.0
(Tom Marler)
TM Data Temporary Storage
Data Transfer and Capture System (DTCS)
V 1.0
IRIG time stamp
Data handling system
Extrapolate missile flyout from 100 meters to go
Transfer shooter, target & missile TSPI data from secondary to primary SCRAMNET loop
BIT3 #412 I/F to EDS (Slot 1)
SCRAMNet Node (Slots 3&4)
IRIG Time Processor BANCOMM bc635VME (Slot 5)
Time stamps missile data coming back
MC860VB/16M Processor (ADCU) (Slot 6)
BIT3 #412 I/F to EDS (Slot 7)
VSB Backplane
MC860VB/16M Processor (DTCS) (Slot 8)
MMI 6346D-64M Memory (DTCS) (Slot 9)
VSB Backplane
Flight Hardware Interface 394-33910 (ADCU) (Slots 11&12)
MMI 6346D-64M Memory (ADCU) (Slot 13)
VMIC 4101 16 Ch. DAC (Ch 0:15) (Slot 16)
VMIC 4101 16 Ch. DAC (Ch 16:31) (Slot 17)
Flight Hardware Interface
10 msec refresh rate
SCRAMNet Node (Slots 18&19)
VME Chassis
E-NET/488
DOF to GPS Simulation Controller
Northern Telecom 2760 GPS Simulator
62.5 MM
External Optical Drive 2x300Mb (1 Gb total with full compression)
TSPI archive for all hardware-in-the-loop data
Trajectory
Missile TM (TTV)
Target TSPI
IRIG time
Missile clock
Gould Ethernet TSPI
SGI IRIS II
IRIX 4.01
E-Net
Simulation Master Computer
Gould 32/9780
CCFEXEC
HWIL S/W
SCRAMNET
Read shooter & target TSPI
File Driven
MTACS Pod
MTACS Pod
Shooter
MTACS Pod
MTACS Pod
4

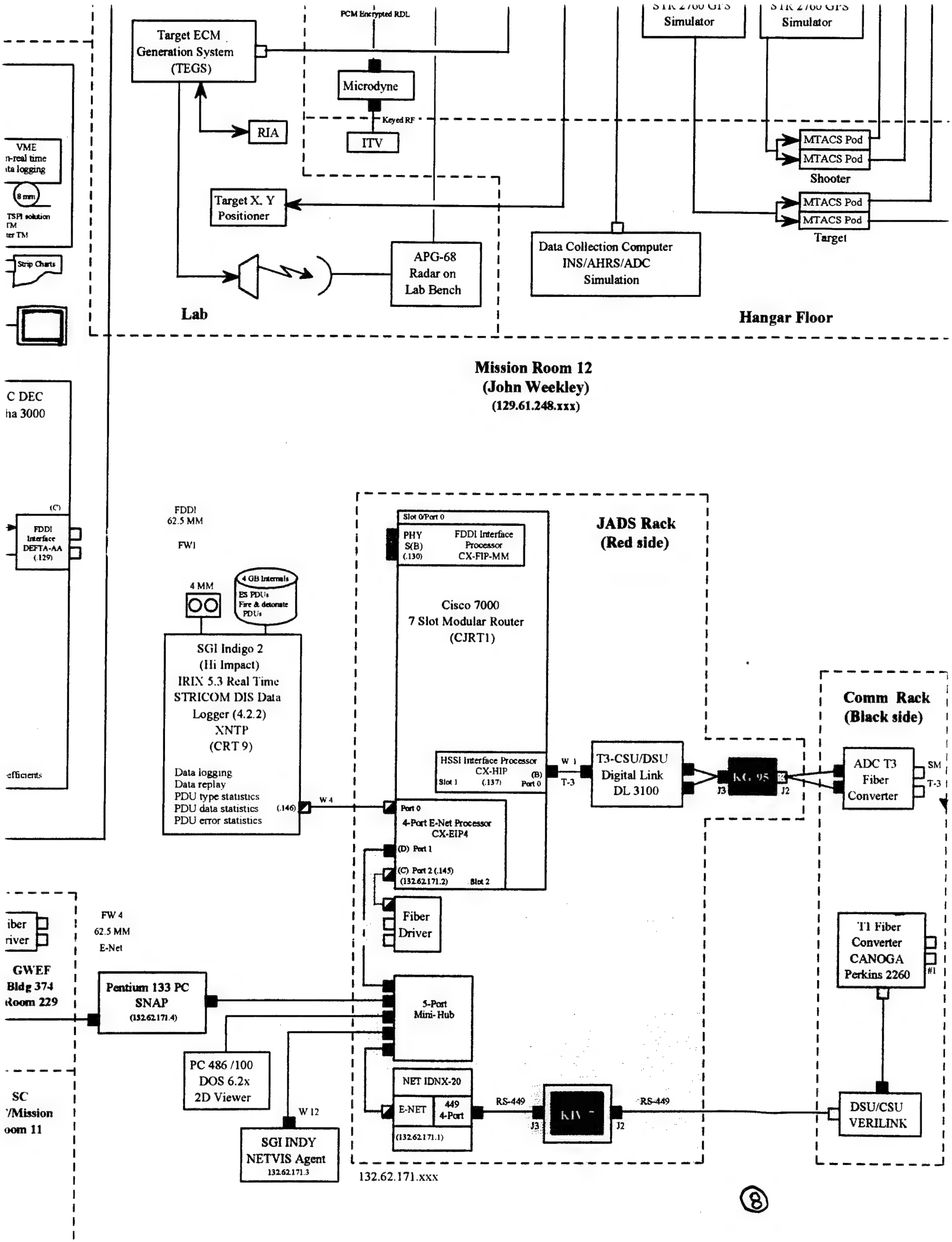


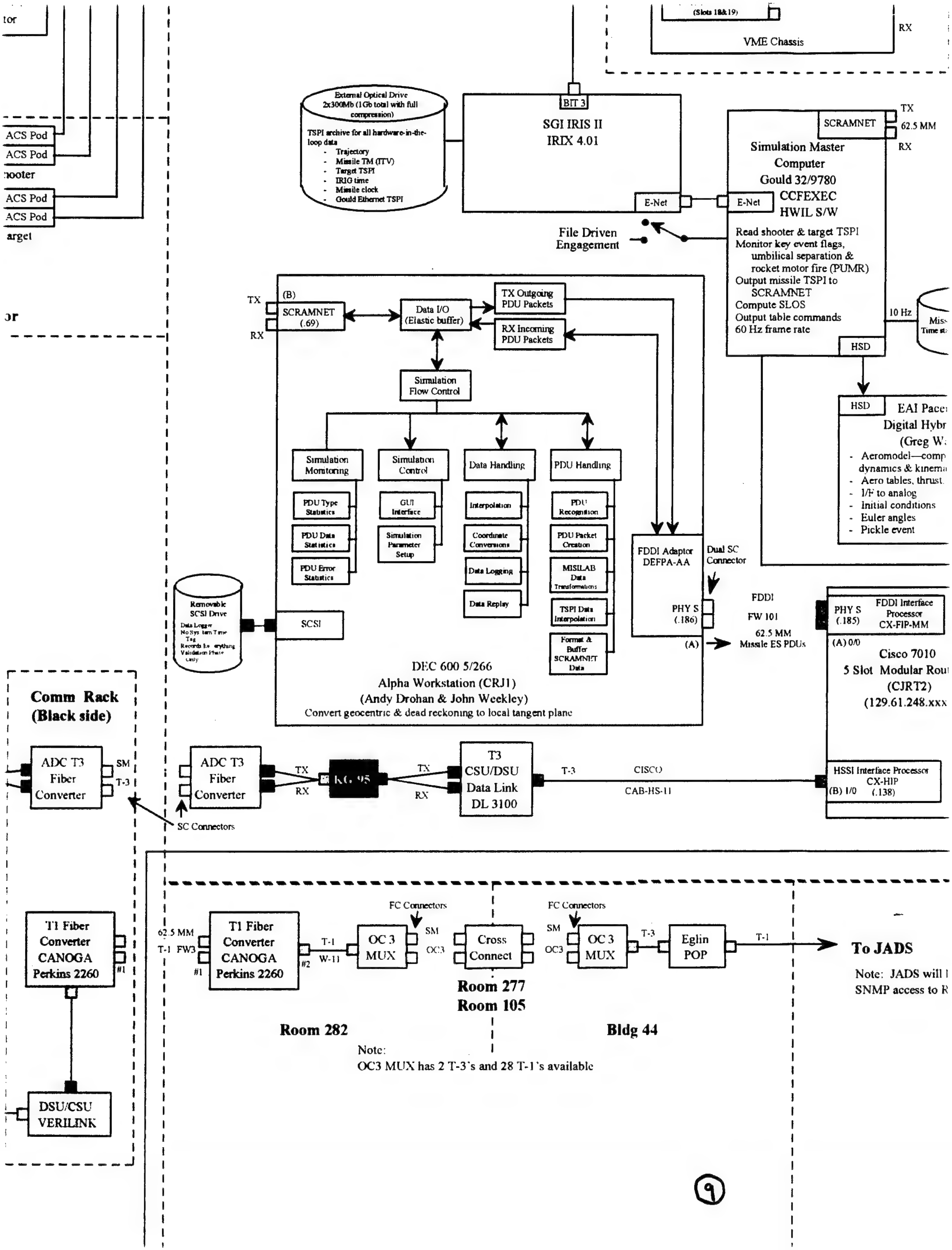
Operand Memory Data & TM (100 Hz)
RS-232/488
486 PC 'Osprey'
PDP-11/44 Emulator
(Doug Ayers)
Downloads tactical software
I/F to microprocessor cards
Emulates UMB & RDL
IRU simulation
Emulates launch aircraft functions
Logical Interface Unit (LIU)/
Extended RAM (XRAM)
GSH-A Test Station
(Doug Ayers)
Missile ECU & batteries
- Powers missile
- Table control & protection
- RDL RF generator controls frequency attenuation
RS-232
1760
Advanced Aircraft Simulation Interface
(AASI)
HPE 1401B VXI Card Cage
100 Hz Frame rate
Register based transfers to DRAM 8 Mb/s
- Block transfers 20 Mb/s
- 600 bytes per frame in 75 µsec
Worst case before umbilical disconnect 6 msec
- Read SCRAMNET & transfer to DRAM 0.75 msec
- Process & partition for I/O & 1553 boards 1.5 msec
- Set up I/O board with umbilical & differential discretes 0.75 msec
- Send targeting & uncertainty data to 1553 board 2 msec
- Receive status msg from 1553 board 1 msec
SBS Dual MIL-STD-1553B
1760 Interface (Slot 12)
Test Point
1760
MIL STD 1760
I/F Adaptor
Digital Multifunction I/O (Slot 10)
Rear Data Link
Bi-directional RDL Sim (Slot 8)
SCRAMNET LX
(2 Mb RAM) (Slot 6)
100 Mb Zip Drive
Executable & Data Transfer (Slots 4&5)
2 Gb Removable SCSI-2
Program & Classified Data (Slots 2&3)
PC Compatible Slot 0 Controller
(National VXI PC-850/133)
Main Test System Controller
(Windows NT)
64 Mb DRAM
16 Mb Windows
16 Mb Program Executable
32 Mb High speed logging for umbilical data (9 minutes @ 100 Hz)
(Slots 0&1)
MISILAB
SCRAMNET
RX
TX
Data Collection Unit (ADCU)
60 CPU Boards (16 MIP)
V 1.0
(Tom Marler)
Data Temporary Storage
er and Capture System (DTCS)
V 1.0
imp
g system
missile flyout from 100 meters to go
ter, target & missile TSPI data from
to primary SCRAMNET loop
/F to EDS (Slot 1)
et Node (Slots 3&4)
Processor
MM
VME
(Slot 5)
B/16M
(ADCU) (Slot 6)
(Slot 7)
/F to EDS
VSB Backplane
VB/16M Processor (DTCS) (Slot 8)
346D-64M Memory (DTCS) (Slot 9)
VSB Backplane
rdware Interface 394-33910 (ADCU)
(Slots 11&12)
46D-64M Memory (ADCU) (Slot 13)
16 Ch DAC
(Slot 16)
16 Ch DAC
(Slot 17)
Flight Hardware Interface
10 msec refresh rate
Net Node
18&19)
VME Chassis
TX
RX
Seeker Digital
Processor
Missile guidance
Watanabe 8 Channel
Linear Corder Mark VII
Strip Charts
Flight Motion
Simulator
Seeker
Hardware
Room 182A
Room 182B
(Wayne Hostillo)
Antenna Array
Signal Distribution
System
Radar Target
Simulator
Range
Delay
Unit
Range
Extent
Unit
RF Generator
Segment
Target Model 1
50 Hz Frame Rate
BIT 3
BIT 3
RF Control System (RFCS)
V 5.0
5 MC860 VB CPU Boards
SCRAMNET
VME Chassis
RX
TX
Sun 4/330 Host
TARGEN 4.0
Generates target scenarios
SGI 4D/310VGX Workstation
IRIX 4.01
SCRAMNET
RX
TX
Simulation Engagement Display System
(SEDS)
Visual representation of missile simulation
3 views simultaneously
- Seeker
- Behind missile
- Missile line of sight
SCRAMNET
TX
62.5 MM
RX
Simulation Master
Computer
Gould 32/9780
CCFEXEC
HWIL S/W
E-Net
5
Room 182C


Fiber Converters (3)
FC Connectors
Bldg 44
FC Connectors
Fiber Converters (3)
90 Mbit/sec MUX
T-3
Bldg 380 Room 146
EMR 8245 SMART Box MUX
PCM
Bldg 380 Room 149
Telemetry & Magnetic Tape (Telemag) Facility
Bit Synchronizers (6)
Clock
Data
KG-66
Fiber Driver (3)
Fiber Driver
KGR-66
HDDR playback includes time
Real time data log 35 msec delayed time stamp
Patch Panel
INS
IRIG Time Code Generator
Strip Charts
Teledyne Telemetry Processing System (TPS)
Time stamp (35 msec delayed)
DR-11W
VAX 8550 Host CT2
APTEC IOC24 I/O Computer
DRE-11
Room 140
PCM DR-11W
Time Aircraft INS
20 Hz
VAX 8650 CR ACFT INS Preprocess
FDDI
Dejitter & synch internal INS clock to IRIG Time stamp data
DRE-11
VAX 8650 CR 2 ACFT INS
Aircraft control page General 2D view
Real time
Aircraft control log
Slant range
Range rate
Bearing
Bearing rate
Chromatic 2D Viewer
Control Room
Bldg 44
DMX - 2003 & MDR-8 Radios
Fiber Converter
Fiber Converter
Fiber Driver (2)
DML-45
Loral ADS-100 Embedded Time
Mission Room 7 (MTACS Control Room)
VAX 8650 CR 3 Multi-object Tracking & Control System (MTACS) GPS-DIS
9 Track
Real Time GPS Reference Receiver
PCL
PCL
DRE-11
PCL-11B
Real Time FDDI
100 Mb/s Token Ring
FDDI
PDP 11/84 VG 3
FDDI
PDP 11/84 Standard Data System Server SDS 3
TSPI Data Processor (TDP)
Geocentric Attitude to ES PDU
10 Hz Solution Rate
VME Bus
IRIG Time
IRIG Time
Disk Controller
Sun SPARC 2
Serial I/F daughter
DR-11/W input I/F
DR-11/W output I/F
Sun SPARC 2 Range I/F Processor
SCSI/E-NET daughter
10 Hz Solution
Sun SPARC 2 Filter (Shooter)
Sun SPARC 2 Filter (Target)
Sun SPARC 2 Smoother (Shooter)
Sun SPARC 2 Smoother (Target)
VME Chassis
Fiber Optic Cable
SCSI-2
MIL-STD 1553
RGB Cable
10Base-2 ThinNet
DB-15
DB-25
DB-37
BNC
RJ-45
MIC FDDI
SCSI-2
Pushdown
ST
Router

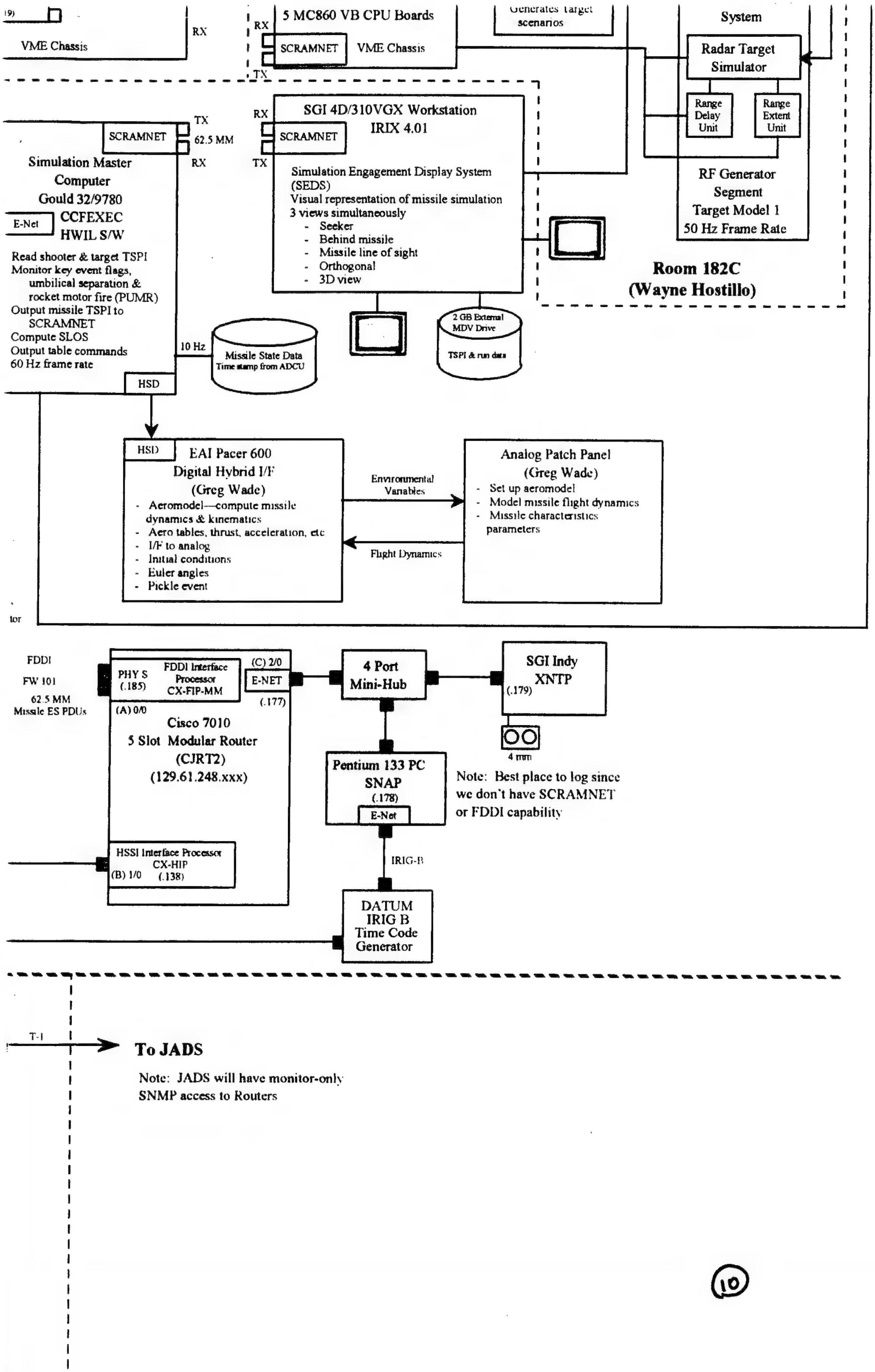


Switch
Switch
DR11-B
RS-232
PDP 11/84
SDS 1
Standard data system server
PCL
FDDI
RS-232
DM-232 Hub
RS-422
19.2 Kb
MicroVAX 3
GPS Pseudo-Range Ground Reference Receiver
Time Code Receiver (TCR)
RS-232
DR11-C
TCR I/F
RS-232
FDDI
PCL
PDP 11/84
VG 4
Calcomp VG4500 (6)
P 11/84
VG 3
Chromatics (4)
Room 147
-11B
Hub
KGR 66
KG 68
KG 68
TTL
TTL
Room 282
LORAL 550
TM Front End
Mainframe Data Rate - 100 Hz
Serial
Serial
Bit sync/decommutation & preprocess
Generate data PDUs
Time correlate
Time stamp
MUX Bus Write
MUX Bus
Bridge
VME
VME
Non-real time data logging
8 mm
Data Loggers
TDP TSPI solution
ITV TM
Shooter TM
E-NET
VTX-2000
X-Windows
Terminal
Strip Charts
E-NET
(.1)(A)
CCC DEC
Alpha 3000
Data Log
MUX Bus data capture
AMRAAM TM to data PDU conversion process
Dejitter program
RX MUX Bus Data (TM/TDP)
(C)
MUX Bus Write
TX Outgoing PDU Packets
Data I/O
RX Incoming PDU Packets
FDDI Interface DEFTA-AA (.129)
TDP Answer Set to PDU Entity State Conversion Process (.65)
Data
Control
Simulation Flow Control/Data Distribution Process
Monitor/Control Display
Simulation Control
PDU Handling
Simulation Parameter Setup
GUI Interface
PDU Recognition
PDU Packet Creation
Kinematic Smoother
(.65)(B)
E-NET
Generate Dead Reckoning Coefficients
DEC DEFAR Fiber Converter
Mission Room 9
(TSPI Control Room)
ECEF TSPI
62.5MM
E-NET
Sun SPARC 2 #1
IPX
Set up and control
Sun SPARC 2 #2
Super Host
TSPI Data Processor (TDP)
Monitor & control
Local tangent plane
Local tangent plane
Full Rate Sensors
TAR
GPS 10 Hz
INS 30 Hz
Radar 10 Hz
Solution 1 Hz
Multiport Fan-Out Transceiver
DEC DEFAR Fiber Converter
DEC DEFAR Fiber Converter
olution
Multiport Fan-Out Transceiver
DEC DEFAR Fiber Converter
E-NET
GWEF
IRIG
Time
IRIG B Receiver
SGI Onyx
Fiber Driver
VDE 160
Transmitter & MUX
GWEF
Bldg 374
Room 229
FW 4
62.5 MM
E-Net
Pent
62.5 MM
VDE 160
Receiver & MUX
SC
CCC/Mission
Room 11
RG-59 Cables
Barco Large Screen Display
7

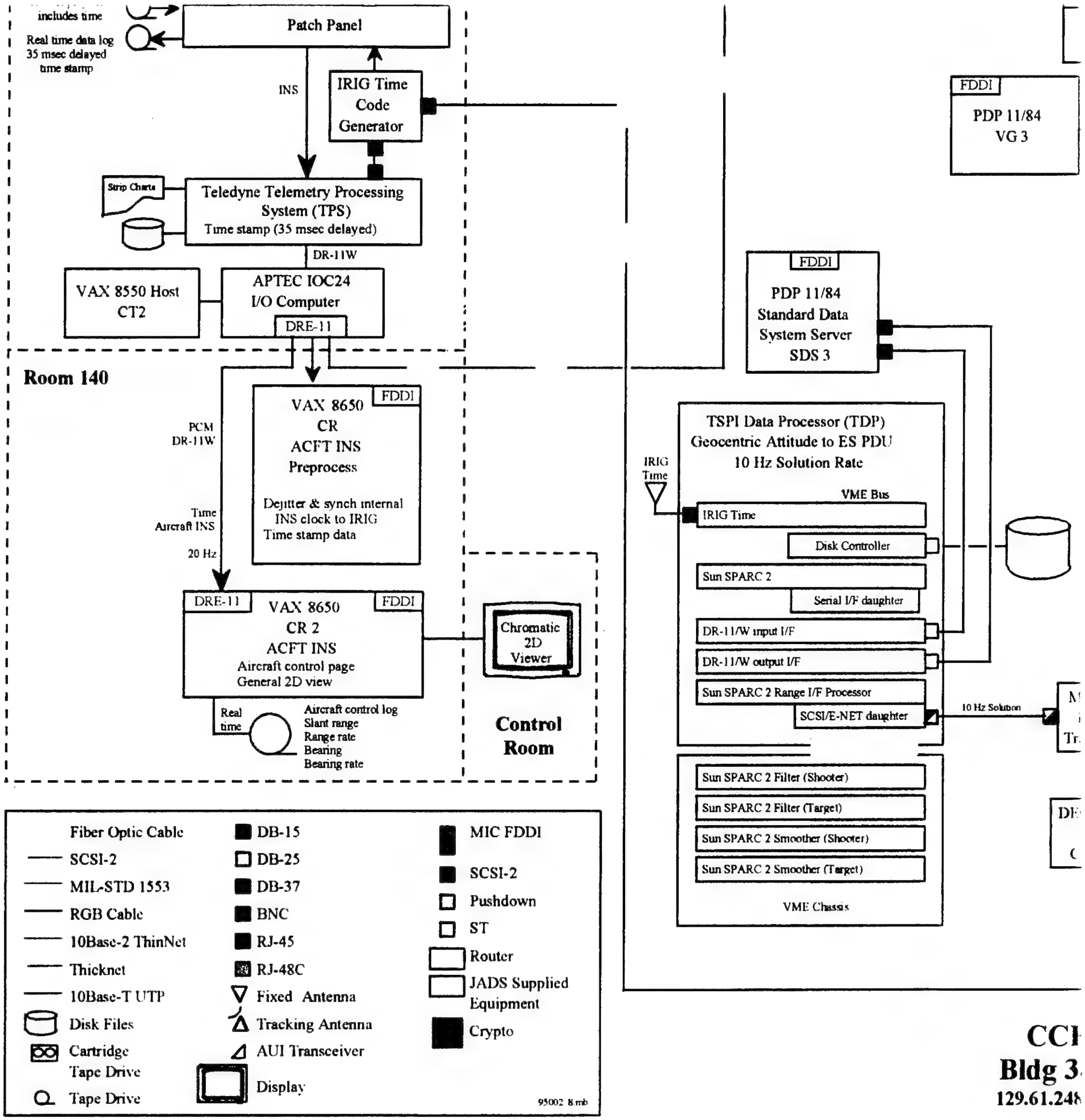

STK 2700 GPS Simulator
STK 2700 GPS Simulator
PCM Encrypted RDL
Target ECM Generation System (TEGS)
Microdyne
Keyed RF
ITV
RIA
VME
n-real time
ita logging
8 mm
TSPI solution
TM
ter TM
Strip Charts
Target X, Y Positioner
APG-68 Radar on Lab Bench
Lab
MTACS Pod
MTACS Pod
Shooter
MTACS Pod
MTACS Pod
Target
Data Collection Computer INS/AHRS/ADC Simulation
Hangar Floor
Mission Room 12
(John Weekley)
(129.61.248.xxx)
C DEC
ha 3000
(C)
FDDI Interface DEFTA-AA (.129)
efficients
FDDI 62.5 MM
FW1
4 MM
4 GB Internals
ES PDUs
Fire & detonate PDUs
SGI Indigo 2
(Hi Impact)
IRIX 5.3 Real Time
STRICOM DIS Data
Logger (4.2.2)
XNTP
(CRT 9)
Data logging
Data replay
PDU type statistics
PDU data statistics
PDU error statistics
(.146)
W 4
JADS Rack
(Red side)
Slot 0/Port 0
PHY S(B) (.130)
FDDI Interface Processor CX-FIP-MM
Cisco 7000
7 Slot Modular Router
(CJRT1)
HSSI Interface Processor CX-HIP
Slot 1
(.137)
(B) Port 0
W 1
T-3
T3-CSU/DSU Digital Link DL 3100
J3
J2
Comm Rack
(Black side)
ADC T3 Fiber Converter
SM
T-3
Port 0
4-Port E-Net Processor CX-EIP4
(D) Port 1
(C) Port 2 (.145)
(132.62.171.2)
Slot 2
Fiber Driver
iber
river
FW 4
62.5 MM
E-Net
GWEF
Bldg 374
Room 229
Pentium 133 PC SNAP (132.62.171.4)
5-Port Mini-Hub
PC 486 /100
DOS 6.2x
2D Viewer
W 12
SGI INDY NETVIS Agent 132.62.171.3
NET IDNX-20
E-NET
449 4-Port
(132.62.171.1)
RS-449
J3
J2
RS-449
T1 Fiber Converter CANOGA Perkins 2260
#1
DSU/CSU VERILINK
SC
/Mission
oom 11
132.62.171.xxx

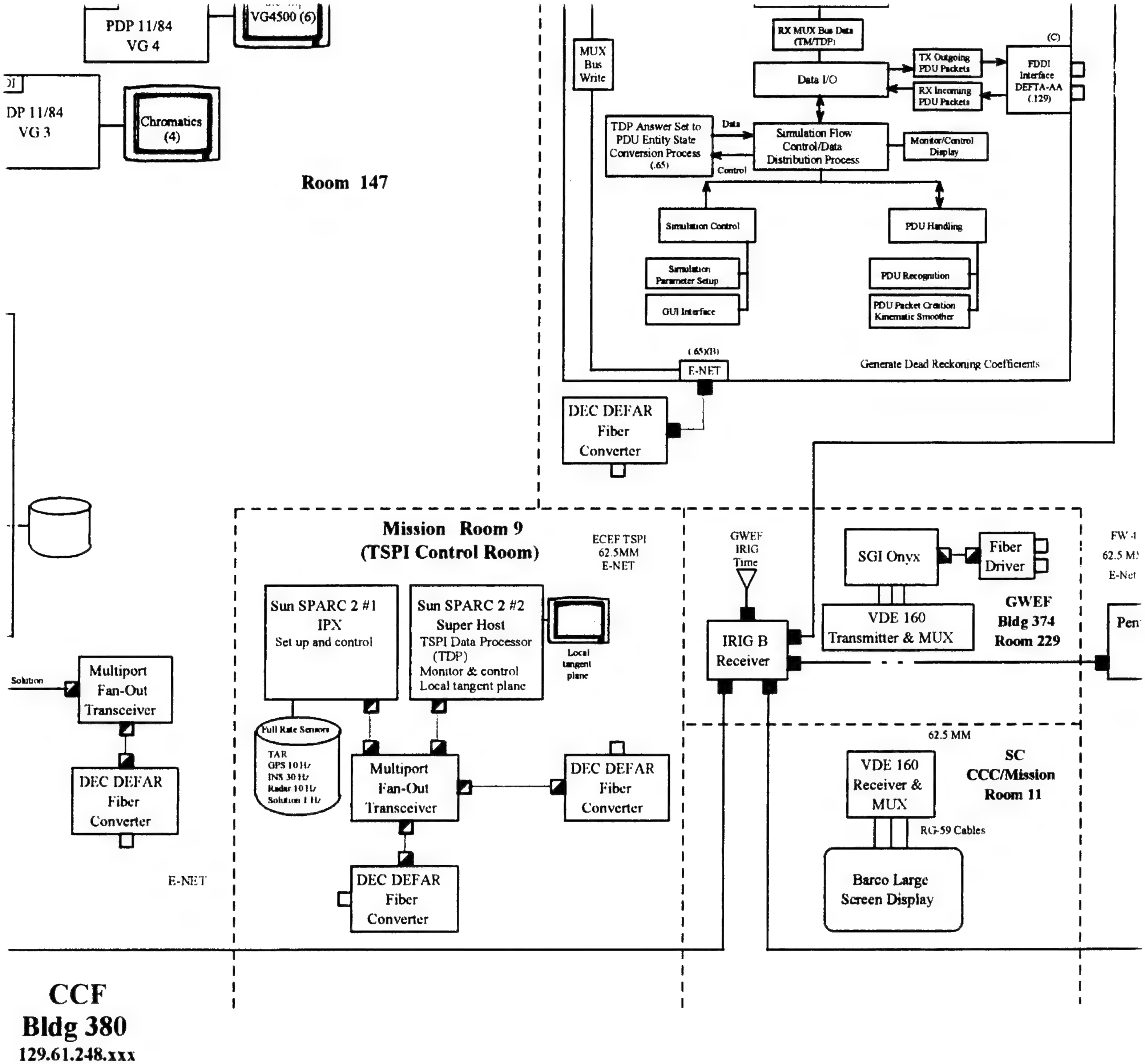


(Slots 18&19)
VME Chassis
RX
External Optical Drive 2x300Mb (1 Gb total with full compression)
TSPI archive for all hardware-in-the-loop data
- Trajectory
- Missile TM (ITV)
- Target TSPI
- IRIG time
- Missile clock
- Gould Ethernet TSPI
BIT 3
SGI IRIS II
IRIX 4.01
E-Net
SCRAMNET
TX
62.5 MM
RX
Simulation Master Computer
Gould 32/9780
CCFEXEC
HWIL S/W
Read shooter & target TSPI
Monitor key event flags, umbilical separation & rocket motor fire (PUMR)
Output missile TSPI to SCRAMNET
Compute SLOS
Output table commands
60 Hz frame rate
HSD
10 Hz
File Driven Engagement
ACS Pod
ACS Pod
ACS Pod
ACS Pod
(B)
SCRAMNET (.69)
Data I/O (Elastic buffer)
TX Outgoing PDU Packets
RX Incoming PDU Packets
Simulation Flow Control
Simulation Monitoring
Simulation Control
Data Handling
PDU Handling
PDU Type Statistics
PDU Data Statistics
PDU Error Statistics
GUI Interface
Simulation Parameter Setup
Interpolation
Coordinate Conversions
Data Logging
Data Replay
PDU Recognition
PDU Packet Creation
MISILAB Data Transformations
TSPI Data Interpolation
Format & Buffer SCRAMNET Data
FDDI Adaptor DEFPA-AA
Dual SC Connector
PHY S (.186)
(A)
FDDI
FW 101
62.5 MM
Missile ES PDUs
Removable SCSI Drive
SCSI
DEC 600 5/266
Alpha Workstation (CRJ1)
(Andy Drohan & John Weekley)
Convert geocentric & dead reckoning to local tangent plane
HSD
EAI Pace
Digital Hybr
(Greg W
- Aeromodel—comp dynamics & kinema
- Aero tables, thrust
- I/F to analog
- Initial conditions
- Euler angles
- Pickle event
PHY S (.185)
FDDI Interface Processor CX-FIP-MM
(A) 0/0
Cisco 7010
5 Slot Modular Rou
(CJRT2)
(129.61.248.xxx
Comm Rack (Black side)
ADC T3 Fiber Converter
SM
T-3
ADC T3 Fiber Converter
TX
RX
KG-95
TX
RX
T3 CSU/DSU Data Link DL 3100
T-3
CISCO
CAB-HS-11
HSSI Interface Processor CX-HIP
(B) 1/0 (.138)
SC Connectors
T1 Fiber Converter CANOGA Perkins 2260
#1
DSU/CSU VERILINK
62.5 MM
T-1 FW3
#1
T1 Fiber Converter CANOGA Perkins 2260
#2
T-1
W-11
FC Connectors
OC 3 MUX
SM
OC3
Cross Connect
FC Connectors
SM
OC3
OC 3 MUX
T-3
Eglin POP
T-1
To JADS
Note: JADS will
SNMP access to R
Room 277
Room 105
Room 282
Bldg 44
Note:
OC3 MUX has 2 T-3's and 28 T-1's available
9

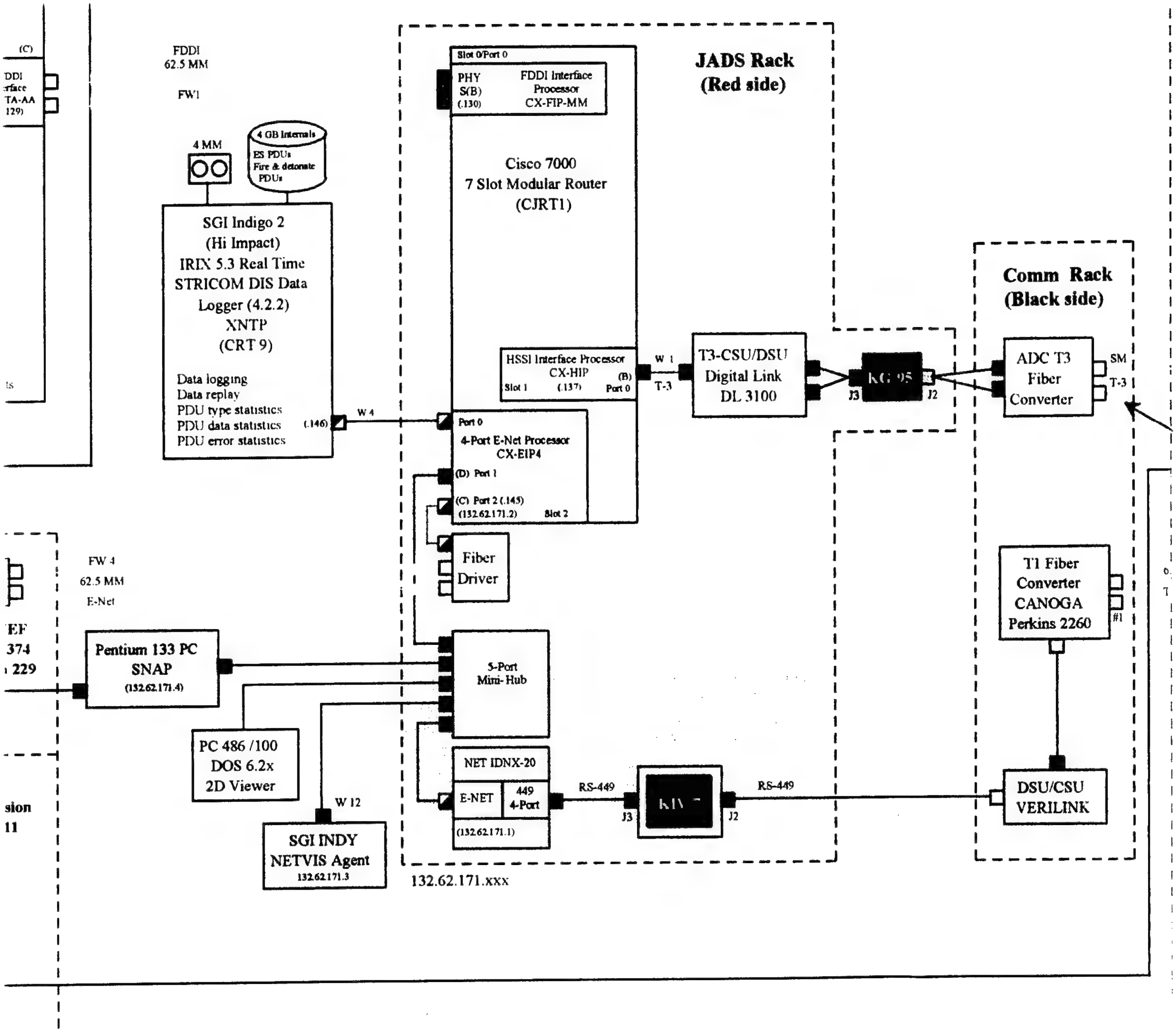


VME Chassis
RX
5 MC860 VB CPU Boards
SCRAMNET
VME Chassis
TX
Generates target scenarios
System
Radar Target Simulator
Range Delay Unit
Range Extent Unit
RF Generator Segment
Target Model 1
50 Hz Frame Rate
Room 182C
(Wayne Hostillo)
SCRAMNET
TX
62.5 MM
RX
Simulation Master Computer
Gould 32/9780
E-Net
CCFEXEC
HWIL S/W
Read shooter & target TSPI
Monitor key event flags, umbilical separation & rocket motor fire (PUMR)
Output missile TSPI to SCRAMNET
Compute SLOS
Output table commands
60 Hz frame rate
HSD
SGI 4D/310VGX Workstation
IRIX 4.01
SCRAMNET
Simulation Engagement Display System (SEDS)
Visual representation of missile simulation
3 views simultaneously
- Seeker
- Behind missile
- Missile line of sight
- Orthogonal
- 3D view
10 Hz
Missile State Data
Time stamp from ADCU
2 GB External MDV Drive
TSPI & run data
HSD
EAI Pacer 600
Digital Hybrid I/F
(Greg Wade)
- Aeromodel—compute missile dynamics & kinematics
- Aero tables, thrust, acceleration, etc
- I/F to analog
- Initial conditions
- Euler angles
- Pickle event
Environmental Variables
Flight Dynamics
Analog Patch Panel
(Greg Wade)
- Set up aeromodel
- Model missile flight dynamics
- Missile characteristics parameters
FDDI
FW 101
62.5 MM
Missile ES PDUs
PHY S (.185)
FDDI Interface Processor CX-FIP-MM
(C) 2/0
E-NET
(.177)
(A) 0/0
Cisco 7010
5 Slot Modular Router
(CJRT2)
(129.61.248.xxx)
HSSI Interface Processor CX-HIP
(B) 1/0 (.138)
4 Port Mini-Hub
SGI Indy XNTP
(.179)
4 mm
Pentium 133 PC
SNAP
(.178)
E-Net
Note: Best place to log since we don't have SCRAMNET or FDDI capability
IRIG-B
DATUM IRIG B Time Code Generator
T-1
To JADS
Note: JADS will have monitor-only SNMP access to Routers

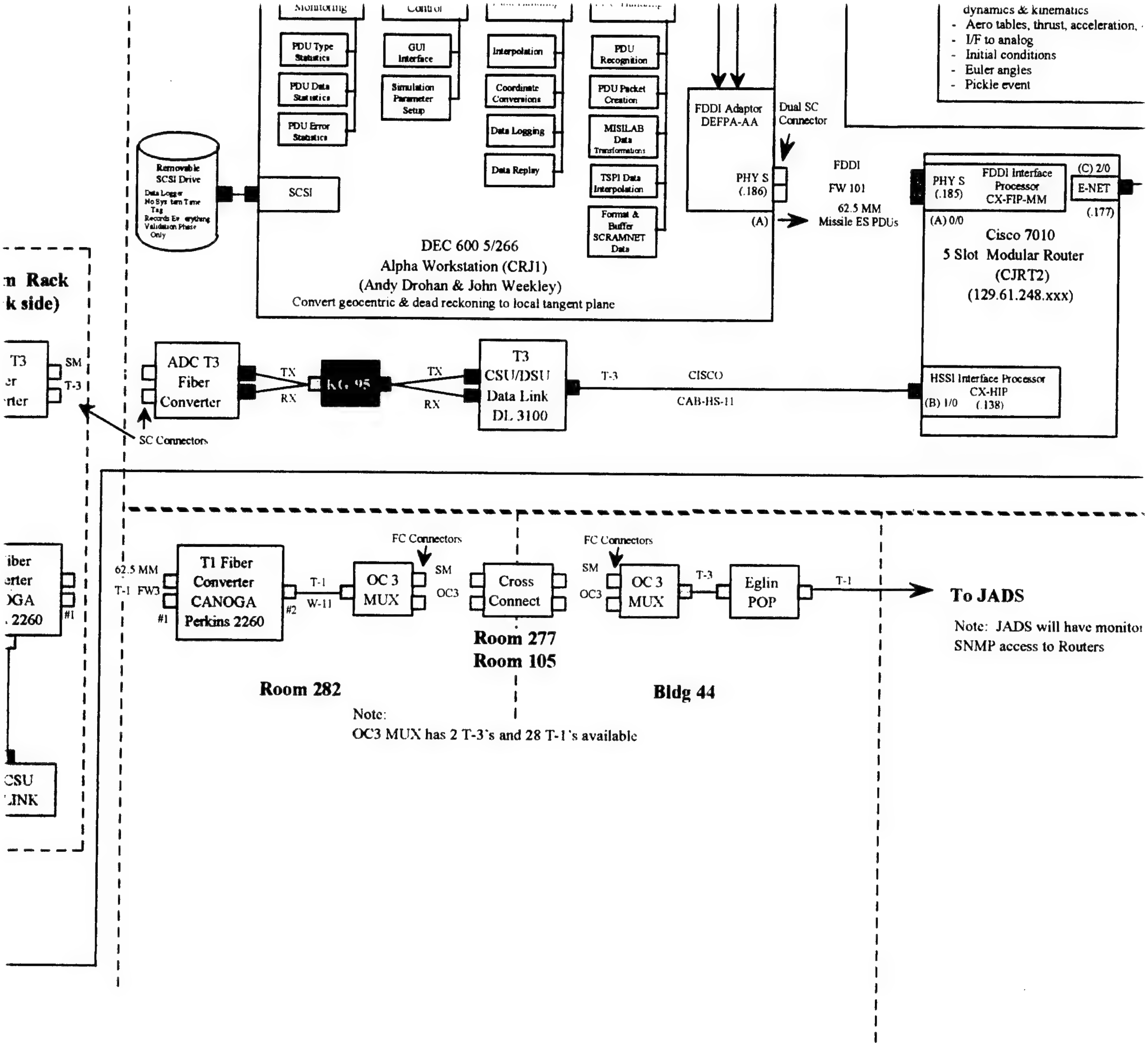

includes time
Real time data log 35 msec delayed time stamp
Patch Panel
INS
IRIG Time Code Generator
Strip Charts
Teledyne Telemetry Processing System (TPS)
Time stamp (35 msec delayed)
DR-11W
VAX 8550 Host CT2
APTEC IOC24 I/O Computer
DRE-11
Room 140
PCM DR-11W
Time Aircraft INS
20 Hz
FDDI
VAX 8650 CR ACFT INS Preprocess
Dejitter & synch internal INS clock to IRIG
Time stamp data
DRE-11
VAX 8650 CR 2 ACFT INS
Aircraft control page
General 2D view
Real time
Aircraft control log
Slant range
Range rate
Bearing
Bearing rate
Chromatic 2D Viewer
Control Room
PDP 11/84 VG 3
PDP 11/84 Standard Data System Server SDS 3
TSPI Data Processor (TDP)
Geocentric Attitude to ES PDU
10 Hz Solution Rate
IRIG Time
VME Bus
IRIG Time
Disk Controller
Sun SPARC 2
Serial I/F daughter
DR-11/W input I/F
DR-11/W output I/F
Sun SPARC 2 Range I/F Processor
SCSI/E-NET daughter
10 Hz Solution
Sun SPARC 2 Filter (Shooter)
Sun SPARC 2 Filter (Target)
Sun SPARC 2 Smoother (Shooter)
Sun SPARC 2 Smoother (Target)
VME Chassis
Fiber Optic Cable
SCSI-2
MIL-STD 1553
RGB Cable
10Base-2 ThinNet
Thicknet
10Base-T UTP
Disk Files
Cartridge Tape Drive
Tape Drive
DB-15
DB-25
DB-37
BNC
RJ-45
RJ-48C
Fixed Antenna
Tracking Antenna
AUI Transceiver
Display
MIC FDDI
SCSI-2
Pushdown
ST
Router
JADS Supplied Equipment
Crypto
95002 8 mb
CCI
Bldg 3
129.61.24

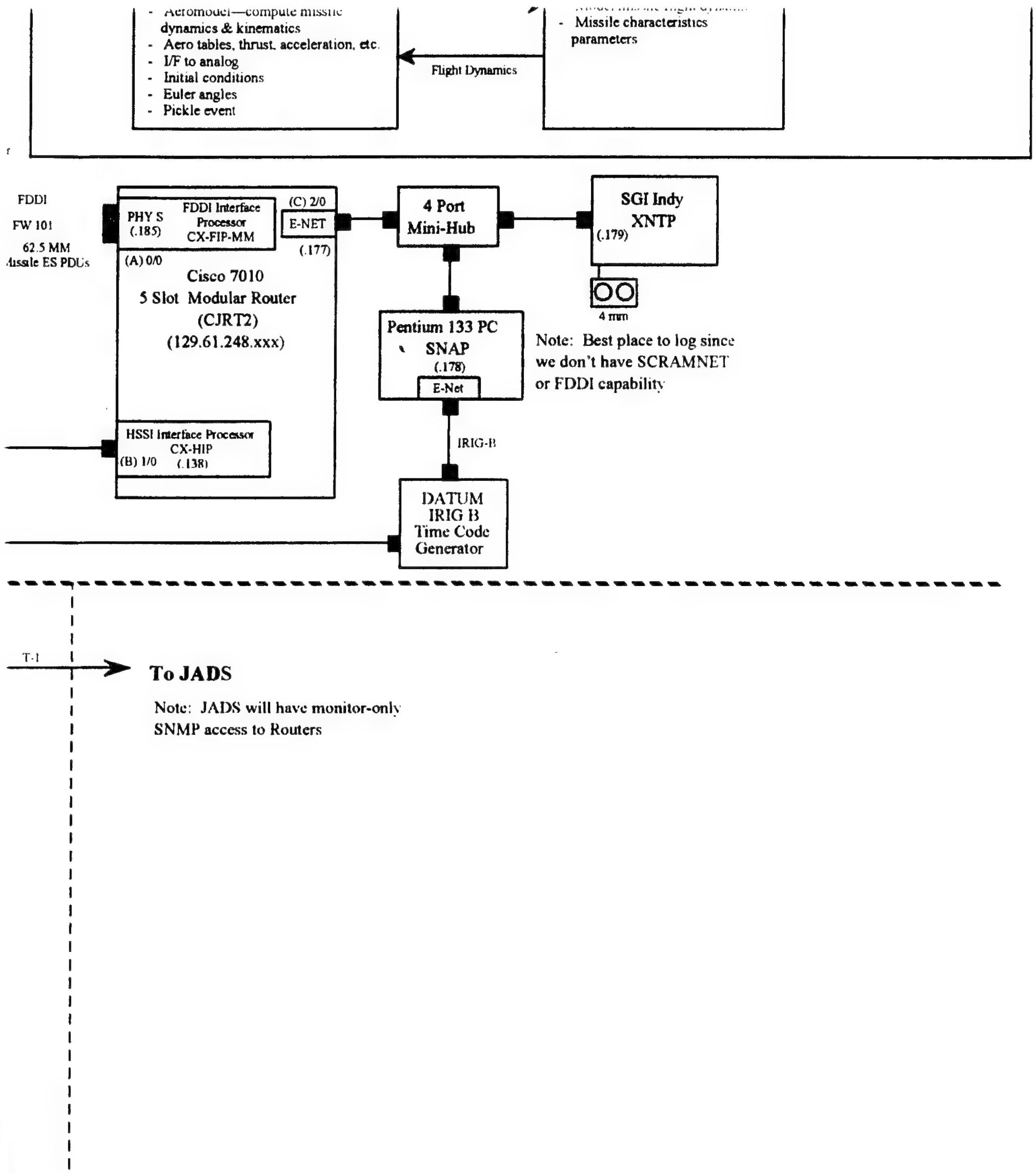

PDP 11/84
VG 4
VG4500 (6)
DP 11/84
VG 3
Chromatics (4)
Room 147
MUX Bus Write
RX MUX Bus Data (TM/TDP)
Data I/O
TX Outgoing PDU Packets
RX Incoming PDU Packets
(C)
FDDI Interface DEFTA-AA (.129)
TDP Answer Set to PDU Entity State Conversion Process (.65)
Data
Control
Simulation Flow Control/Data Distribution Process
Monitor/Control Display
Simulation Control
PDU Handling
Simulation Parameter Setup
GUI Interface
PDU Recognition
PDU Packet Creation Kinematic Smoother
(.65)(B)
E-NET
Generate Dead Reckoning Coefficients
DEC DEFAR Fiber Converter
Mission Room 9
(TSPI Control Room)
ECEF TSPI
62.5MM
E-NET
GWEF IRIG Time
SGI Onyx
Fiber Driver
VDE 160 Transmitter & MUX
GWEF
Bldg 374
Room 229
FW 4
62.5 M
E-Net
Pen
Sun SPARC 2 #1
IPX
Set up and control
Sun SPARC 2 #2
Super Host
TSPI Data Processor (TDP)
Monitor & control
Local tangent plane
Local tangent plane
IRIG B Receiver
Solution
Multiport Fan-Out Transceiver
Full Rate Sensors
TAR
GPS 10 Hz
INS 30 Hz
Radar 10 Hz
Solution 1 Hz
Multiport Fan-Out Transceiver
DEC DEFAR Fiber Converter
DEC DEFAR Fiber Converter
62.5 MM
SC
CCC/Mission
Room 11
VDE 160 Receiver & MUX
RG-59 Cables
Barco Large Screen Display
E-NET
DEC DEFAR Fiber Converter
CCF
Bldg 380
129.61.248.xxx

12



FDDI
62.5 MM
FW1
4 MM
4 GB Internals
ES PDUs
Fire & detonate PDUs
SGI Indigo 2
(Hi Impact)
IRIX 5.3 Real Time
STRICOM DIS Data
Logger (4.2.2)
XNTP
(CRT 9)
Data logging
Data replay
PDU type statistics
PDU data statistics
PDU error statistics
(.146)
W 4
JADS Rack
(Red side)
Slot 0/Port 0
PHY
S(B)
(.130)
FDDI Interface Processor CX-FIP-MM
Cisco 7000
7 Slot Modular Router
(CJRT1)
HSSI Interface Processor
CX-HIP
(B)
Slot 1
(.137)
Port 0
W 1
T-3
T3-CSU/DSU
Digital Link
DL 3100
KG-95
J3
J2
Port 0
4-Port E-Net Processor
CX-EIP4
(D) Port 1
(C) Port 2 (.145)
(132.62.171.2)
Slot 2
Fiber
Driver
Comm Rack
(Black side)
ADC T3
Fiber
Converter
SM
T-3
T1 Fiber
Converter
CANOGA
Perkins 2260
#1
FW 4
62.5 MM
E-Net
Pentium 133 PC
SNAP
(132.62.171.4)
5-Port
Mini-Hub
PC 486 /100
DOS 6.2x
2D Viewer
W 12
SGI INDY
NETVIS Agent
132.62.171.3
NET IDNX-20
E-NET
449
4-Port
(132.62.171.1)
RS-449
KIV-7
J3
J2
RS-449
DSU/CSU
VERILINK
132.62.171.xxx

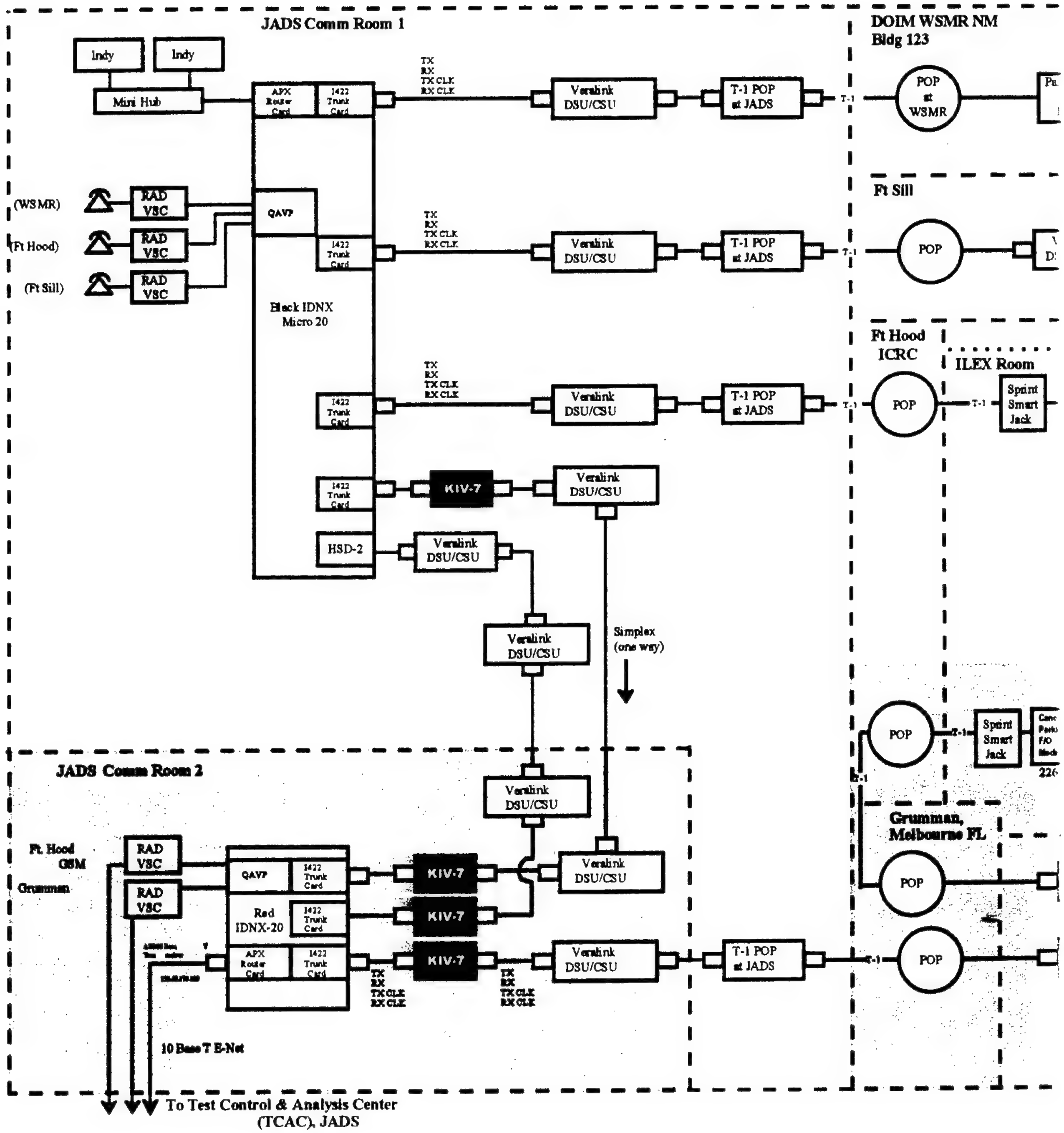

PDU Type Statistics
PDU Data Statistics
PDU Error Statistics
GUI Interface
Simulation Parameter Setup
Interpolation
Coordinate Conversions
Data Logging
Data Replay
PDU Recognition
PDU Packet Creation
MISILAB Data Transformations
TSPI Data Interpolation
Format & Buffer SCRAMNET Data
dynamics & kinematics
- Aero tables, thrust, acceleration,
- I/F to analog
- Initial conditions
- Euler angles
- Pickle event
Removable SCSI Drive
SCSI
FDDI Adaptor DEFPA-AA
Dual SC Connector
PHY S (.186)
(A)
FDDI
FW 101
62.5 MM
Missile ES PDUs
PHY S (.185)
FDDI Interface Processor CX-FIP-MM
(C) 2/0
E-NET
(.177)
(A) 0/0
Cisco 7010
5 Slot Modular Router
(CJRT2)
(129.61.248.xxx)
DEC 600 5/266
Alpha Workstation (CRJ1)
(Andy Drohan & John Weekley)
Convert geocentric & dead reckoning to local tangent plane
Rack
k side)
T3
SM
T-3
ADC T3 Fiber Converter
TX
RX
T3 CSU/DSU Data Link DL 3100
T-3
CISCO
CAB-HS-11
HSSI Interface Processor CX-HIP
(B) 1/0 (.138)
SC Connectors
62.5 MM
T-1 FW3
#1
T1 Fiber Converter CANOGA Perkins 2260
#2
T-1
W-11
FC Connectors
SM
OC3
OC 3 MUX
Cross Connect
Room 277
Room 105
OC 3 MUX
T-3
Eglin POP
T-1
To JADS
Note: JADS will have monitor SNMP access to Routers
Room 282
Bldg 44
Note:
OC3 MUX has 2 T-3's and 28 T-1's available
CSU
LINK



- Aeromodel—compute missile dynamics & kinematics
- Aero tables, thrust, acceleration, etc.
- I/F to analog
- Initial conditions
- Euler angles
- Pickle event
Flight Dynamics
- Missile characteristics parameters
FDDI
FW 101
62.5 MM
Missile ES PDUs
PHY S (.185)
FDDI Interface Processor CX-FIP-MM
(C) 2/0
E-NET
(.177)
(A) 0/0
Cisco 7010
5 Slot Modular Router
(CJRT2)
(129.61.248.xxx)
HSSI Interface Processor CX-HIP
(B) 1/0 (.138)
4 Port Mini-Hub
SGI Indy XNTP
(.179)
4 mm
Pentium 133 PC
SNAP
(.178)
E-Net
Note: Best place to log since we don't have SCRAMNET or FDDI capability
IRIG-B
DATUM IRIG B Time Code Generator
T-1
To JADS
Note: JADS will have monitor-only SNMP access to Routers

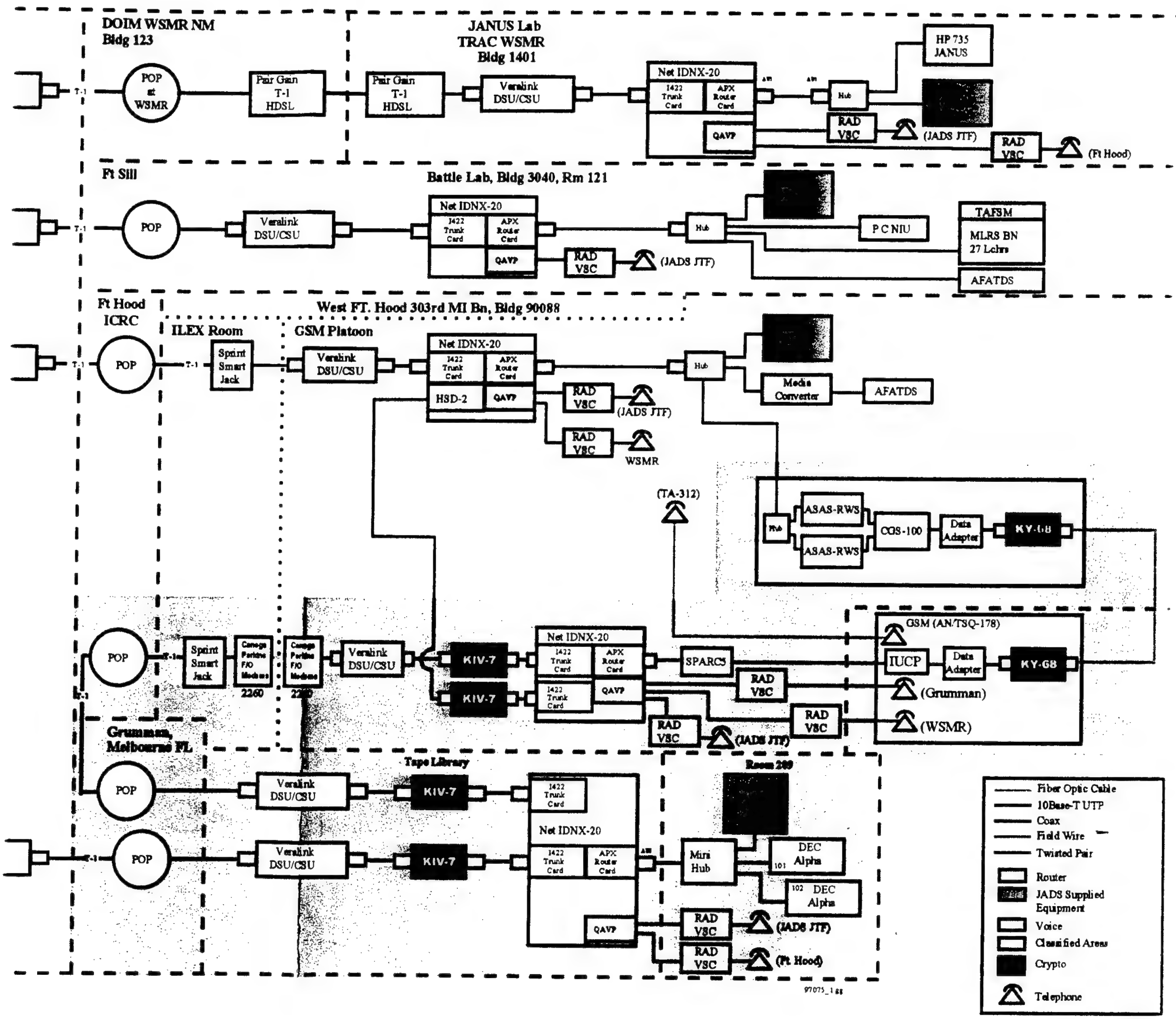
End To En

Phase

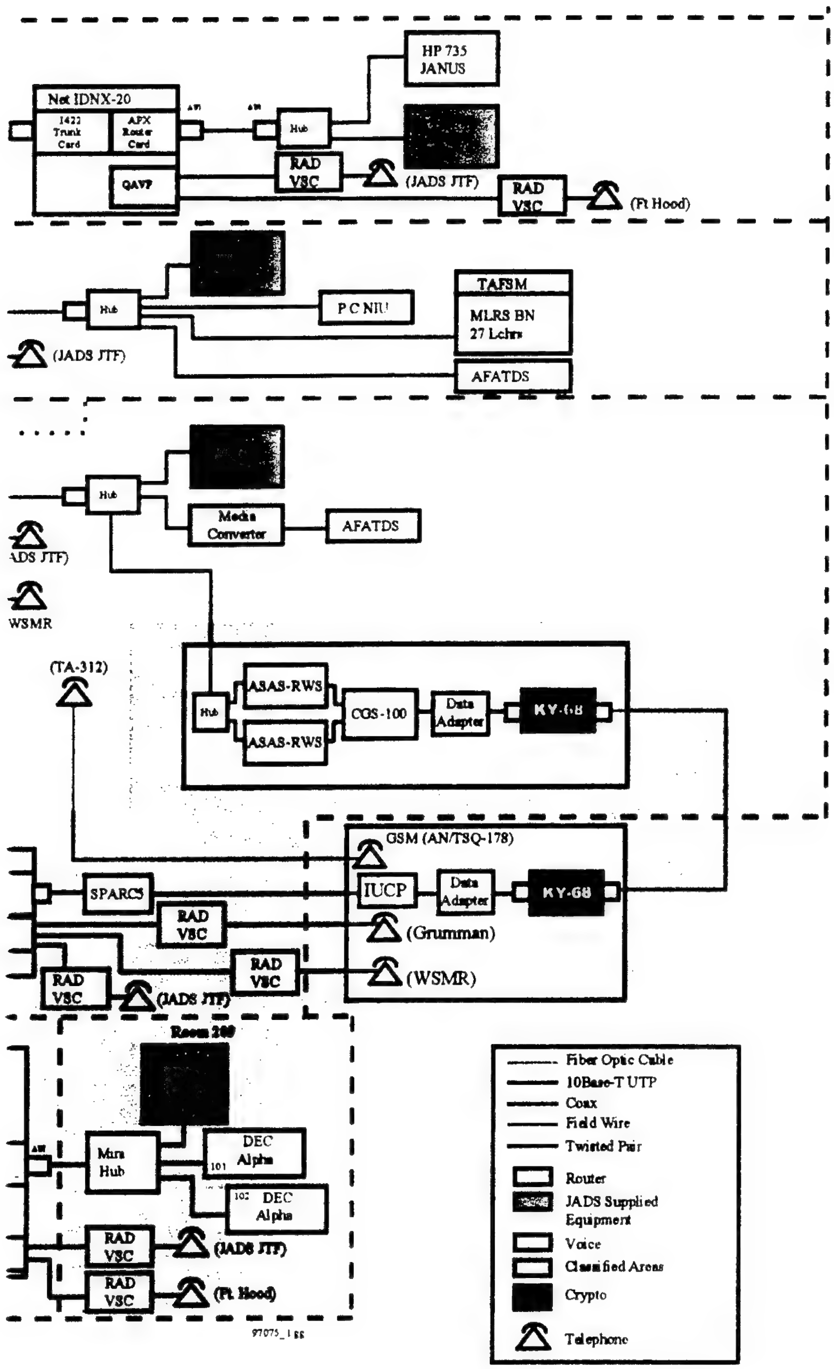


d To End Network

Phase 2 & 4



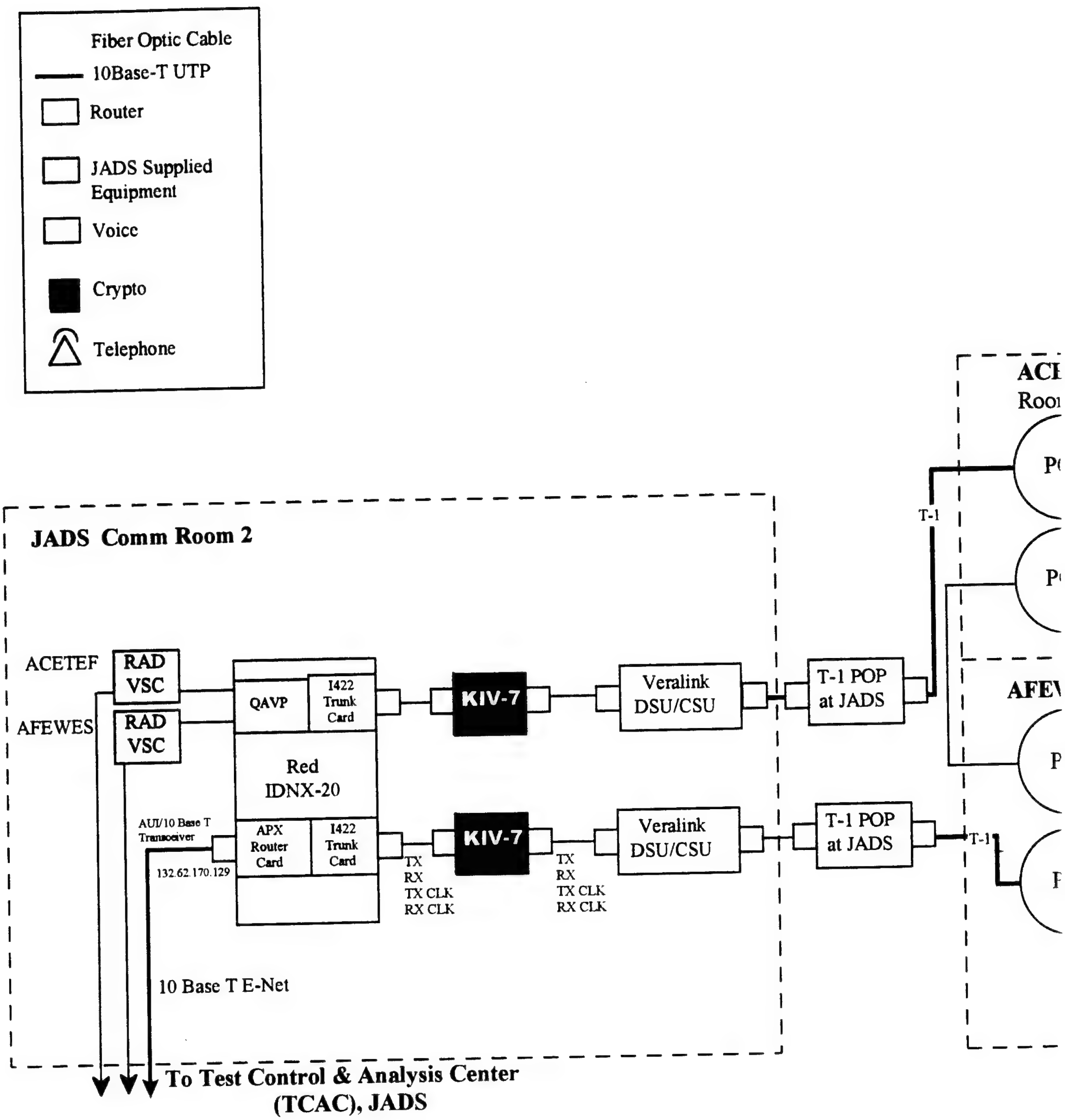
14 July 1999



14 July 1999

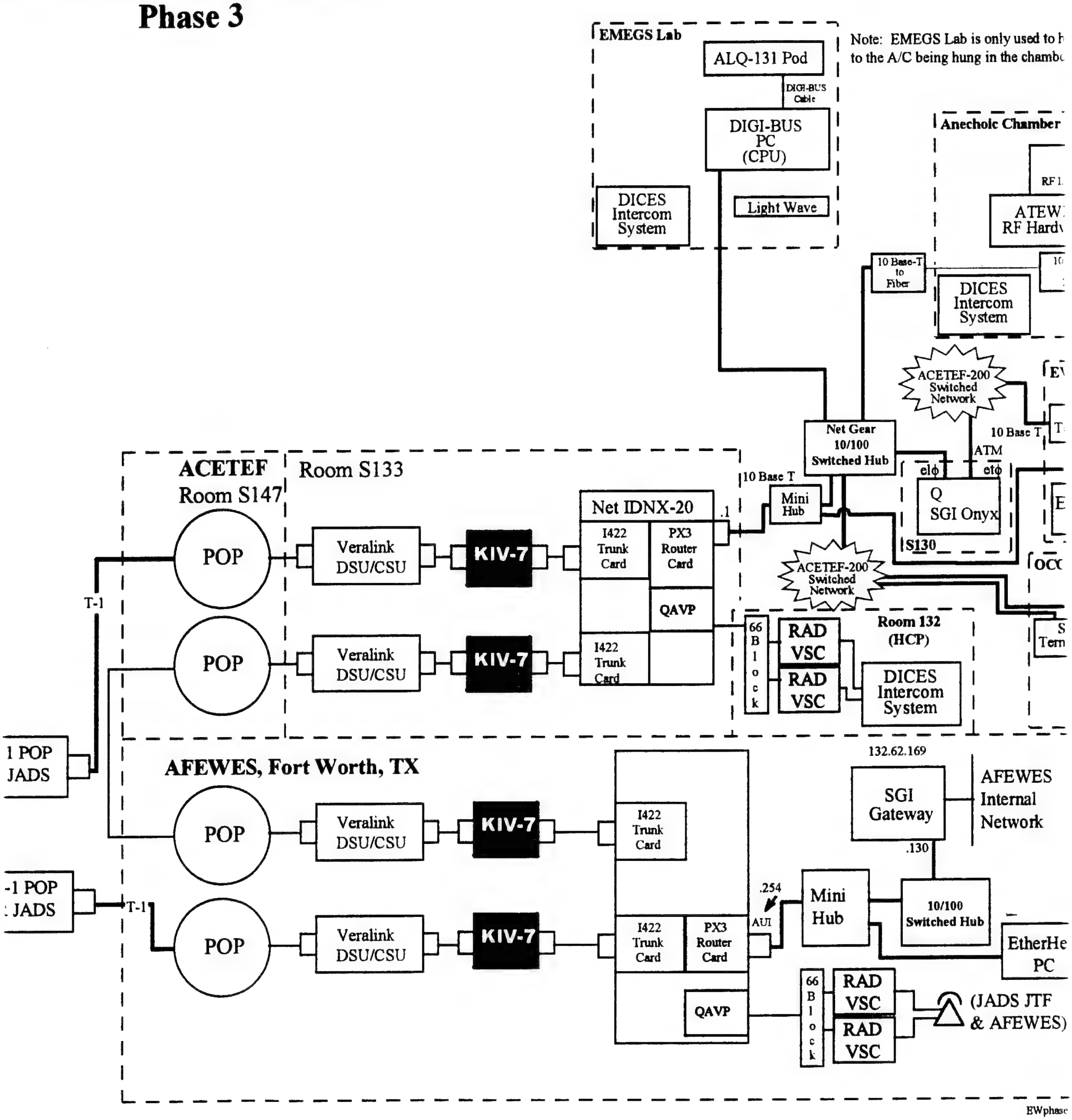
③

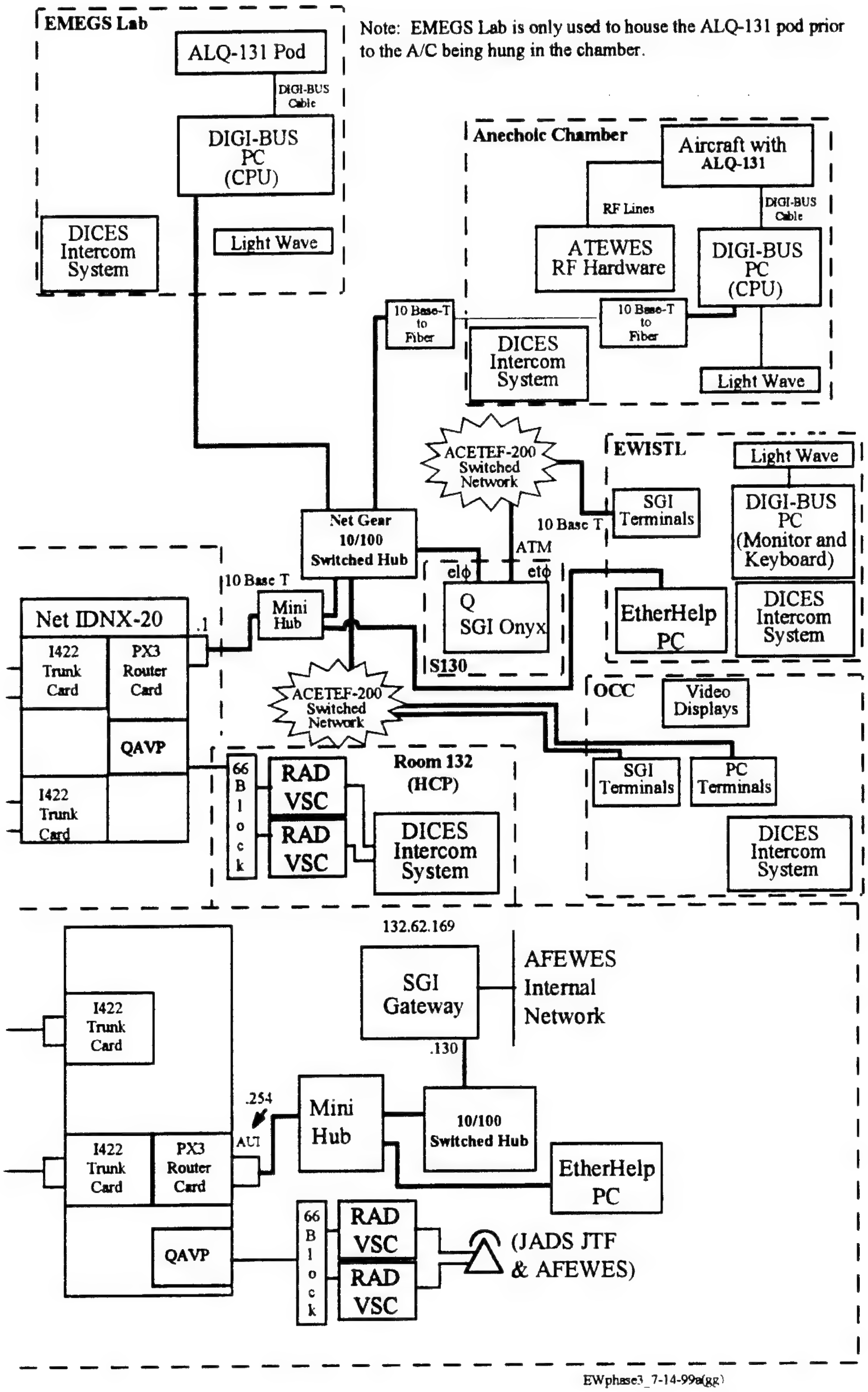
EW Test Netwo
Phase



1

EW Test Network Diagram
Phase 3





EMEGS Lab
ALQ-131 Pod
DIGI-BUS Cable
DIGI-BUS PC (CPU)
DICES Intercom System
Light Wave
Note: EMEGS Lab is only used to house the ALQ-131 pod prior to the A/C being hung in the chamber.
Anechoic Chamber
Aircraft with ALQ-131
RF Lines
DIGI-BUS Cable
ATEWES RF Hardware
DIGI-BUS PC (CPU)
10 Base-T to Fiber
10 Base-T to Fiber
DICES Intercom System
Light Wave
ACETEF-200 Switched Network
EWISTL
Light Wave
SGI Terminals
DIGI-BUS PC (Monitor and Keyboard)
10 Base T
ATM
Net Gear 10/100 Switched Hub
elϕ
etϕ
Q SGI Onyx
S130
EtherHelp PC
DICES Intercom System
10 Base T
Mini Hub
Net IDNX-20
.1
1422 Trunk Card
PX3 Router Card
QAVP
1422 Trunk Card
ACETEF-200 Switched Network
OCC
Video Displays
SGI Terminals
PC Terminals
DICES Intercom System
66 Block
RAD VSC
RAD VSC
Room 132 (HCP)
DICES Intercom System
132.62.169
SGI Gateway
AFEWES Internal Network
.130
1422 Trunk Card
.254
AUI
Mini Hub
10/100 Switched Hub
1422 Trunk Card
PX3 Router Card
EtherHelp PC
QAVP
66 Block
RAD VSC
RAD VSC
(JADS JTF & AFEWES)
EWphase3_7-14-99a(gg)

Appendix B

Characterization of DSI ATM Backbone

for

JADS Traffic

MP 99W0000083VSR

MITRE PAPER

Characterization of DSI ATM Backbone for JADS Traffic

April 1999

S. Chakravorty
P. Feighery

MITRE
Washington C3 Center
McLean, Virginia

Table of Contents

Section 1

Overview

In order to investigate the utility of Advanced Distributed Simulation (ADS) for Test and Evaluation (T&E) applications, the Office of the Secretary of Defense (OSD) chartered the Joint Advanced Distribution Simulation (JADS) Joint Test and Evaluation (JT&E) program. Identification of ADS constraints and methodologies when used for T&E, and requirements for ADS systems to better support T&E in the future are also part of the JADS charter[1].

The JADS JT&E project consists of three multi-phased test programs: the System Integration Test (SIT), End-to-End (ETE) test, and finally Electronic Warfare (EW) test. For each phase of a given test program, there is an associated test scenario that defines a prescribed set of interactions among the program entities. For JADS T&E efforts, a key element of the test program is the communications infrastructure that supports the execution of a test scenario.

MITRE was tasked to determine the network latency JADS sites would incur if they were connected to the DSI network which is a recently modernized network meant to support T&E requirements such as those represented by the SIT, ETE and EW tests. For this latency determination, various tests were conducted by MITRE in coordination with the DSI staff. The JADS program office identified three test sites: Albuquerque, Forth Worth, and Patuxent River. This paper briefly reviews the tests performed and analyzes the results. It also shows how the methodology used in the analysis to determine the latency between these sites could also be used to determine the latency that other JADS sites would experience.

The paper is developed in the following way. First, a background for the tasks is presented. This is followed by assumptions made, and the tools and methodology adopted for the tests. The DSI topologies are then described including the proposed network connectivities to the JADS sites. The information gathered from the tests is then analyzed and latency estimates presented for the JADS site connectivities. Finally, the conclusions are presented.

---

1 This information is provided from other JADS reports. For more information, see JADS web page: www.jads.abq.com/html/jads.

Section 2

Background

The DSI network backbone is an Asynchronous Transfer Mode (ATM) based network. At the local subnet level, the network contains devices called *aggregators* that can be used to concatenate User Datagram Protocol (UDP) based multicast traffic to increase the utilization of the network. To perform this function, these aggregators delay multicast traffic to a configuration amount (default is 10 msec). This analysis assumes that the aggregator is set to zero, that is, there is no delay. The network can also use the network protocol, Resource Reservation Protocol (RSVP), to partition the available bandwidth to separate guaranteed slots dedicated to particular applications[2].

The test plan adopted for this study characterizes the DSI network in terms of throughput and round trip delay. Point to note is that the methodology presented here can be followed to determine the minimum latency for current and future JADS applications connected via the DSI network.

Actual delay an application will incur depends however on many factors including host configuration, application configuration, and background traffic.

Some of these factors are explained below.

a. Host Configuration

The way a networked host is configured affects the performance of applications hosted on that machine. For example, hosts use a parameter called the Maximum Transmission Unit (MTU) for each network interface. The MTU determines the largest frame size that can be transmitted on the network. The MTU affects the transmission efficiency of data packets in that larger the MTU, better the throughput. Another example is the TCP default window size for both the local and remote hosts. This parameter and the end-to-end delay determine the maximum amount of data TCP can have within the network.

b. Application Configuration

For network applications exhibiting performance problems, the network itself is not always the bottleneck. Processing time for applications to spawn processes to handle incoming requests or to handle other physical resources (i.e., access to a disk array) may be the limiting

---

2 This feature was not however used for the tests since there was no requirement to do so.

resource. A system level performance analysis for a particular application may be required to determine how to improve the performance.

c. Background Network Traffic

All connectionless networks, including the DSI network, share their resources among all users of the system. The amount of background traffic from other users of the DSI network will affect the amount of resources that a JADS application can use. The performance tests presented here assume that the network is idle and that test applications can consume all resources necessary.

The three JADS sites evaluated for performance based on the tests are Air Combat Environment Test and Evaluation Facility (ACETEF) in Patuxent River, Maryland, Air Force Electronic Warfare Environment Simulator (AFEWES) in Fort Worth, Texas, and the Test Control and Analysis Center (TCAC) in Albuquerque, New Mexico.

2.1 Assumptions

After an examination of the current DSI topology, the following assumptions were made:

- For JADS sites at Albuquerque and Fort Worth to connect to each other via the DSI backbone, they would be connected via T1 links to the DSI backbone site at Kelly, Texas.
- Similarly, the site at Patuxent River would be connected via a T1 link to the DSI backbone at the Pentagon.

Section 3

Test Tools

The following sections describe the various test tools used for the tests.

3.1 *ping*

The network utility *ping* is used to determine both network's connectivity and round trip delay. This utility uses the Internet Control Message Protocol (ICMP) *echo_request* packet to elicit an ICMP's *echo_response* packet. The utility *ping* reports the number of *pings* sent and the responses received along with the round trip delay through the network. To calculate the latency, one needs simply divide the round trip delay by two. The *ping* utility is standard on Unix operating systems and Cisco routers. It is also provided on Microsoft Windows environments. An example follows.

3.1.1 End-to-End Test from Host x at Site X to Host y at Site Y - *ping* Test

3.1.1.1 Test Objective

The objective of this test is to determine the end to end delay throughput and latency through the network.

3.1.1.2 Test Procedure

The *ping* utility is used to gather data on end-to-end delay. Host x at site X pings host y at site Y 10,000 times. The command format is:

ping –s y.Y 500 10000

3.1.1.3 Results/Analysis

The results provide an indication of route trip delay and the corresponding variance; dividing by 2 provides one way delay. These results also indicate how many of the packets were lost (either due to congestion or corruption) in the network. The output at the sender should look like the following.

ping merit.edu: 492 data bytes

500 bytes from merit.edu (198.108.1.42): icmp_seq=0. time=96. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=1. time=83. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=2. time=93. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=3. time=74. msec

500 bytes from merit.edu (198.108.1.42): icmp_seq=4. time=82. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=5. time=102. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=6. time=99. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=7. time=92. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=8. time=99. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=9. time=84. msec
500 bytes from merit.edu (198.108.1.42): icmp_seq=10. time=82. msec

. . . .

. . . .

----merit.edu *ping* Statistics----

500 packets transmitted, 500 packets received, 0% packet loss
round-trip (ms) min/avg/max = 73/89/102

Note: The first data point (i.e., packet with ICMP sequence number 0) should be ignored because of possible interaction with DNS lookup or ARPing.

3.2 *traceroute*

The network utility *traceroute* is used to trace the path of a packet from its source through a network to its destination. This utility sends a series of UDP packets each increasing Internet Protocol (IP) Time-To-Live field. It operates by trying to illicit ICMP *time_exceeded* packets from intermediate gateways. When this ICMP packet is received, the originating host notes this including the delay, increases the TTL by one, and sends the series of UDP packets again. This continues until the remote host responds. The result is a list of machines the packet traverses and the hop-by-hop round trip network delay. To calculate the latency one need only divide the round trip delay by two. An example follows.

3.2.1 End to End Test from Host x at Site X to Host y at Site Y - *traceroute* Test

3.2.1.1 Test Objective

The objective of this test is to determine the cumulative delay of a packet as it systematically traverses the network.

3.2.1.2 Test Procedure

The *traceroute* utility is used to gather data on end-to-end delay. Host x at site X performs a *traceroute* to host y at site Y. The command format is:

traceroute y.Y

3.2.1.3 Results/Analysis

The results provide an indication of route trip delay from the host to each site at the packet traverses the network; dividing by 2 will provide a one way delay. The delay should be examined for any anomalies.

The following provides a sample output:

traceroute to merit.edu (198.108.1.42), 30 hops max, 40 byte packets

1. w157gw.mitre.org (128.29.31.254) 1 msec 1 msec 2 msec
2. restgw.mitre.org (128.29.217.254) 7 msec 2 msec 1 msec
3. westgw.mitre.org (128.29.1.1) 8 msec 7 msec 9 msec
4. emailgw.mitre.org (128.29.18.247) 8 msec 8 msec 8 msec
5. mwfw1gw.mitre.org (198.76.174.254) 9 msec 8 msec 8 msec
6. mwbogw.mitre.org (198.76.173.254) 9 msec 9 msec 12 msec
7. 205.128.152.254 (205.128.152.254) 12 msec 11 msec 10 msec
8. s8-0.washdc1-cr2.bbnplanet.net (4.0.148.33) 37 msec 44 msec 31 msec
9. fa2-0-0.washdc1-br2.bbnplanet.net (4.0.1.177) 29 msec 38 msec 53 msec
10. p3-0.vienna1-nbr3.bbnplanet.net (4.0.1.90) 32 msec 29 msec 71 msec
11. p1-0.vienna1-nbr2.bbnplanet.net (4.0.5.45) 45 msec 23 msec 50 msec
12. p5-0-0.vienna1-br1.bbnplanet.net (4.0.5.50) 40 msec 43 msec 39 msec
13. core6-hssi6-0-0.Washington.cw.net (206.157.77.217) 41 msec 35 msec 21 msec
14. bordercore2.NorthRoyalton.cw.net (166.48.224.1) 50 msec 73 msec 80 msec
15. merit.NorthRoyalton.cw.net (166.48.225.250) 73 msec 51 msec 65 msec
16. 198.108.22.201 (198.108.22.201) 66 msec 70 msec 50 msec
17. merit.edu (198.108.1.42) 70 msec 87 msec 75 msec

Section 4

Test Methodology

In the DSI network, like in all packet switched networks, end sites are interconnected via the network fabric which in this case is the DSI ATM backbone. To determine the round trip delay between any two end sites, the delay between each intermediate router that connects the two sites must be known. These values are then summed to obtain the total round trip delays. To obtain one way latency, the round trip delay is divided by 2.

Four DSI end sites were selected to mimic distances between the given three JADS sites. The DSI sites chosen were Ft. Bliss, TX; Vicksburg, MS; Ft. Eustis, VA; Ft. Leavenworth, KS.

The test methodology for the tests comprised gathering performance data from the four DSI test sites - both from the black and red sides of the end-site subnets.

With the aid of the DSI Network Operation Center (NOC) at Columbus, Ohio, hop-by-hop round trip test measurements were made for the DSI sites using the *traceroute* utility. Using the measurements obtained from the tests and extrapolating for distances based on the network topology, the delay for the JADS sites were estimated.

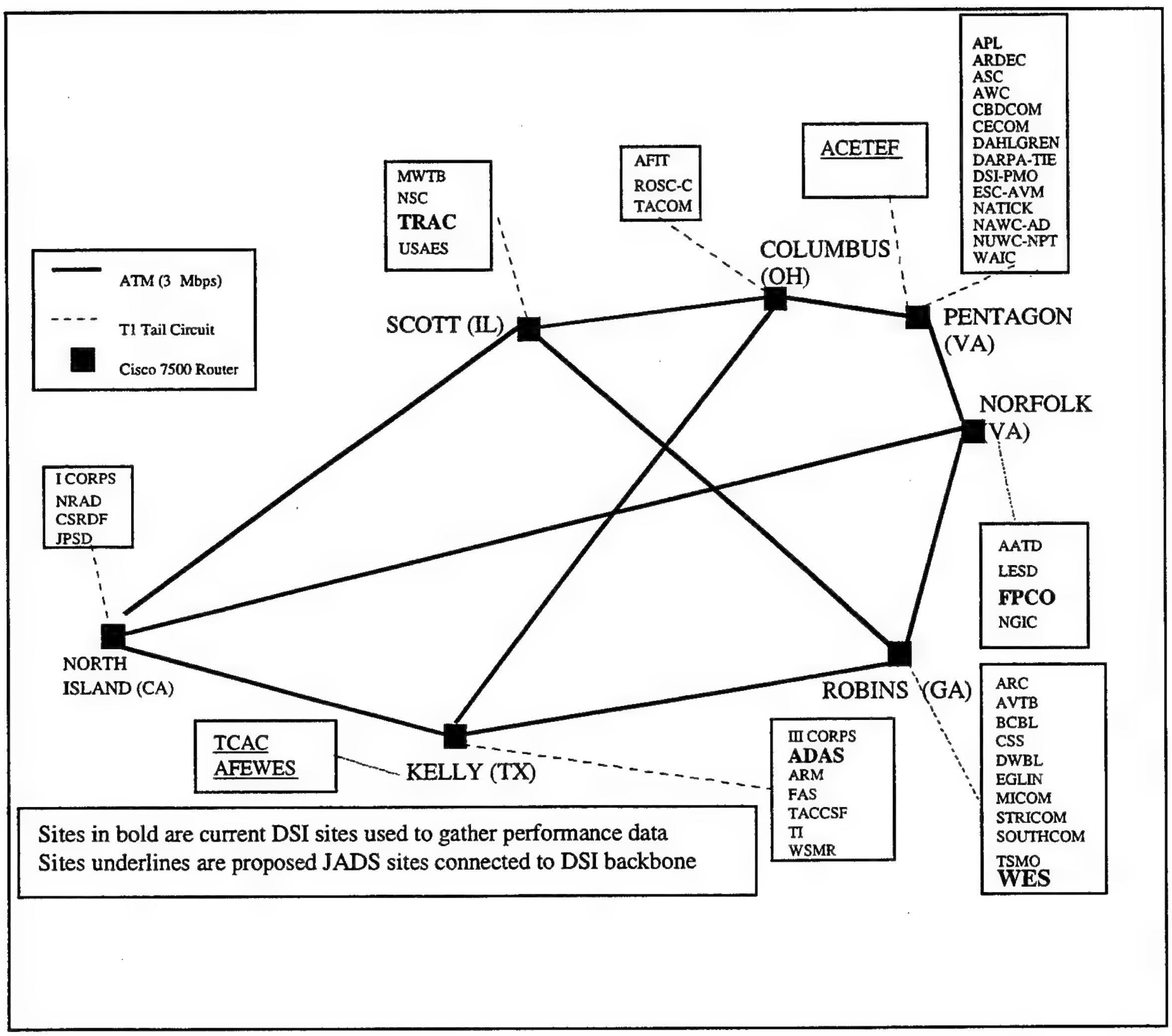
For the *ping* tests, a packet size of 500 bytes was chosen and 10,000 samples for each test was gathered. The Columbus NOC sent a series of *ping* packets (for both the classified and unclassified sides of the network) to the four sample sites already on the DSI network.

In all charts showing the test results, the distances reflect the routes of how the packets traverse the network and not how the crow flies.

Section 5

DSI Backbone Topology

The diagram below shows the current DSI network. The network contains seven backbone sites connected via the ATM running at 3Mbps. The connections between backbone sites were chosen so that a maximum of two backbone hops are needed to connect any two sites. The other sites labeled with boxes are connected to the DSI backbone via a T1 link running at 1.544 Mbps.

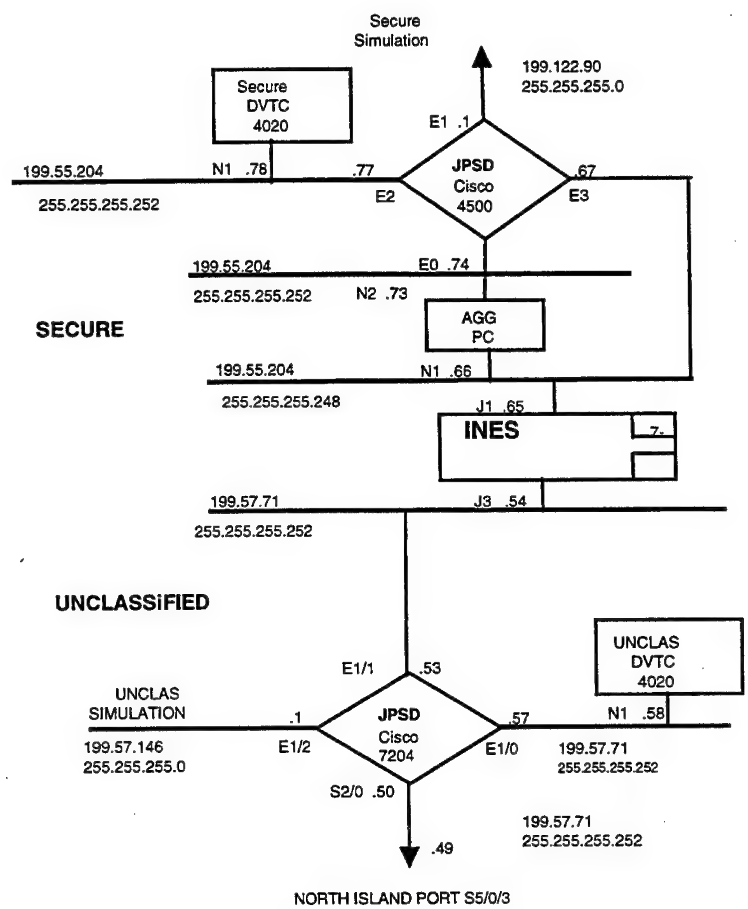


Section 6

Typical Site Topology

The diagram here shows a typical DSI site configuration.

Figure 6-1. Typical DSI Site Configuration



Section 7

Analysis from *ping* tests Between Columbus and the Four Sample Sites

The following chart contains the results of the ping tests from Columbus to the four sample sites currently connected to the DSI network. The average values are of particular interest. The maximum values are usually from the first sample that contains time required for both ARPing and DNS look-up, hence can be ignored.

Ping Tests
Packet Size: 500
Number Packets: 10000

				Black Side				Red Side		
Source	**Destination**	**Distance**	**DSI SITE**	**min**	**ave**	**max**		**min**	**ave**	**max**
Columbus	Ft. Bliss, TX	1750	ADAS	88	90	212		136	144	360
Columbus	Vicksburg, MS	1402	WES	88	98	192		152	159	328
Columbus	Ft. Eustis, VA	650	FPCO	48	50	102		94	104	240
Columbus	Ft Leavenworth, KS	720	TRAC	36	37	172		84	92	224

Note: Distance is in miles.
Note: Roundtrip delay is in msec.

The additional delay when data is sent over the classified link is also available from the above chart. It can be determined that traversing the classified link adds approximately 56 msec of delay to the transmission. This increased delay is mainly due to the processing of INES to encrypt/decrypt data.

Section 8

Analysis from *traceroute* tests Between Columbus and the Three Sample Sites

The following three charts contain sample results from the *traceroute* utility. The utility *traceroute* provides hop-by-hop round trip delay information based on the distance/link type-tuple. For example, the average round trip delay to the site's boundary router via Ethernet is approximately 2 msec. Additionally, as shown in the first chart in Section 8.1 below, to traverse from Scott, IL to Robins GA, a distance of 552 miles, over the DSI ATM backbone running at 3 Mbps, a round trip delay of 24 msec is accrued. To traverse from Robins, GA to Vicksburg, MS, which is a distance of 800 miles over a T1 link, a round trip delay of 52 msec is accrued, and so on. Summarizing, the following information can be obtained from *traceroute*:

- The path of the packet through the network
- The corresponding IP address
- The approximate distance between the sites (this was gathered from the website mapquest.com)
- The round trip delay between the next-hop sites
- The total incurred round trip delay through the network

In the charts, the city/next hop columns show the router location/corresponding IP address the packet travels from source to destination. The distance columns contain the distance in miles from the previous router to that location. The delay column contains the delay in milliseconds for between that router and the previous router. Finally the total delay column is the cumulative delay in milliseconds.

8.1 *traceroute* Test Between Columbus and Vicksburg

The following chart contains the results from the *traceroute* utility from Columbus to Vicksburg, MS.

Source: Columbus, OH **Destination: Vicksburg, MS**

City	Next Hop	Distance	Delay	Total Delay
Columbus, OH	199.57.70.25	0	2	2
Scott, IL	199.57.64.86	420	14	16
Robins, GA	199.57.64.113	552	24	40
Vicksburg, MS	199.57.67.92	800	52	92

Source: Columbus, OH **Destination: Ft. Bliss, TX**

City	Next Hop	Distance	Delay	Total Delay
Columbus, OH	199.57.70.25	0	2	2
Kelly, TX	199.57.64.86	1050	38	40
Ft. Bliss, TX	199.57.68.2	700	40	80

Note: Distance is in msec.
Note: Roundtrip delay is in msec.

8.3 *traceroute* Test Between Columbus and Ft. Eustis

The following chart contains the results from the traceroute utility from Columbus to Ft. Eustis, VA.

Source: Columbus, OH **Destination: Ft. Eustis, VA**

City	Next Hop	Distance	Delay	Total Delay
Columbus, OH	199.57.70.25	0	2	2
Pentagon, DC	199.57.64.97	420	28	30
Norfolk, VA	199.57.64.92	200	8	38
Ft. Eustis, VA	199.57.66.26	30	4	42

Source: Columbus, OH **Destination: Ft. Leavenworth, KS**

City	Next Hop	Distance	Delay	Total Delay
Columbus, OH	199.57.70.25	0	2	2
Scott, IL	199.57.64.38	300	14	16
Ft. Leavenworth, KS	199.57.69.28	300	12	28

Note: Distance is in miles.

Note: Roundtrip delay is in msec.

Section 9

Network Delay

The network delay estimates are summarized in this section.

9.1 Estimates Albuquerque to Ft. Worth Through the DSI Network

The following chart describes the path and delay between the JADS sites at Albuquerque, NM and Ft. Worth, TX.

Source: Albuquerque, NM
Destination: Ft. Worth, TX

City	Link	Distance	Delay	Total Delay
Albuquerque, NM	Local	0	2	2
Kelly, TX	T1	782	48	50
Ft. Worth, TX	T1	77	7	57

Note: Distance in miles.
Note: Roundtrip delay in msec.

The total round trip delay is 57 msec. If the data between these two sites were to be sent classified through the INES an additional round trip delay of 54 msec should be added.

9.2 Network Delay Estimate: Albuquerque to Patuxent River Through the DSI Network

The following chart describes the path and delay between the JADS sites at Albuquerque, NM and Patuxent River, MD.

Source: Albuquerque, NM
Destination: Patuxent River, MD

City	Link	Distance	Delay	Total Delay
Albuquerque, NM	Local	0	2	2
Kelly, TX	T1	782	48	50
Columbus, OH	ATM BB	1050	38	88
Pentagon, DC.	ATM BB	420	28	116
Patuxent River, MD	T1	33	4	120

Note: Distance in miles.

Note: Roundtrip delay in msec.

through the INES, an additional round-trip delay of 56 msec should be added.

Section 10

Conclusions

The traffic from Albuquerque, NM to Fort Worth, TX will not traverse the DSI backbone. Traffic will not need to utilize the higher speed DSI ATM backbone since a direct connection will be more efficient.

However, traffic from Albuquerque, NM to Patuxent River, MD will traverse the DSI backbone. This traffic will utilize the services of the higher speed DSI ATM backbone. If the DSI in the future decides to upgrade the backbone from 3Mbps to a high speed, the traffic may gain some added benefits from greater available bandwidth in the DSI.

The same type of analysis can be used to obtain the probable latency that other JADS sites would obtain if connected to the DSI backbone. The steps would include:

- Determine the point of contact (nearest DSI backbone router) to the JADS site. A T1 link would possibly be used to connect the site
- Determine the probable path from source to destination on the DSI backbone
- Given the line type (either T1 or DSI ATM backbone) and the distance for each next hop, determine the probable round-trip delay as in the charts shown above
- Sum up the results

Finally, to more accurately determine the delay and throughput an actual traffic would experience, other tests to mimic the traffic may be used. These tests would require a greater level of participation from current DSI sites than what was needed for these tests.

Appendix C

A Study
of the
Defense Simulation Internet (DSI)
for the
Joint Advanced Distributed Simulation
Project

WN 98W000032

MITRE REPORT

A Study of the Defense Simulation Internet (DSI) for the Joint Advanced Distributed Simulation (JADS) Project

April 1998

Devaraj Sahu

MITRE

Washington C³ Center
McLean, Virginia

Abstract

This report investigates the feasibility of the recently upgraded Defense Simulation Internet (DSI) network to support Test and Evaluation (T&E) requirements such as the Joint Advanced Distributed Simulation (JADS) phase two end-to-end (ETE) test. It reviews the features associated with the DSI and discusses how the DSI could be used to support JADS ETE T&E efforts.

The DSI provides for bandwidth reservation among its user sites through the use of standards-based Resource ReSerVation Protocol (RSVP). Multicasting is supported so that packets in a distributed simulation are efficiently forwarded. Security is provided by Improved Network Encryption System (INES) boxes built by the Motorola Corporation. Desktop Video Teleconferencing (DVTC) applications can be used among limited number of sites in secure or non-secure mode.

A JADS Phase two ETE test configuration for T&E is discussed and a potential configuration for running this test over DSI is presented. Because of the throughput limitations of the INESs (maximum two-way throughput being 1200 Kbits per second), it is suggested that running JADS ETE phase two tests over the DSI is not a viable option at the present time.

Table of Contents

Section 1

1. INTRODUCTION

The Joint Advanced Distribution Simulation (JADS) program is chartered by the Office of the Secretary of Defense (OSD) to investigate the utility of Advanced Distributed Simulation (ADS) for Test and Evaluation (T&E) applications. JADS has also been asked to identify ADS constraints and methodologies when used for T&E and to identify requirements for ADS systems to better support T&E in the future (for more information, see their web page: www.jads.abq.com/html/jads).

The JADS Joint T&E project consists of three multi-phased test programs: the System Integration Test (SIT), End-to-End (ETE) test, and finally Electronic Warfare (EW) test. The SIT test has been scheduled to run from 1995 through 1998 and the EW and ETE tests will run through 1999. For each phase of a given test program, there is an associated test scenario that defines a prescribed set of interactions among the program entities. For JADS T&E efforts, a key element of the test program is the communications infrastructure that supports the execution of a test scenario.

The JADS Test Director has requested that MITRE investigate the feasibility of the recently modernized Defense Simulation Internet (DSI) to support T&E requirements, such as those represented by the SIT, ETE, and EW tests. In response, MITRE's Networking and Communications Engineering Center initiated a study of the upgraded DSI and its potential impact on JADS-based T&E. This paper reviews the features associated with the DSI and looks at one phase of the JADS ETE test program and discusses how DSI could be used to support this test. This paper also examines the cost and performance implications of using the DSI in the test.

1.1 BACKGROUND

The DSI is a network that allows distributed simulations from all branches of the military to interoperate. It is owned by the Defense Information Systems Agency (DISA). The old DSI (Phase I) wide area network (WAN) consisted of out-dated equipment such as Bolt Beranek and Newman (BBN) T/20 routers and proprietary implementations of the Streams Protocol, Version II (ST II). The modernized Phase II DSI replaced these with state of the art equipment and standards-based commercial products.

1.2 PURPOSE

In this report, the technical characteristics of the modernized DSI network are examined in detail and include the standards-based protocols and applications available in the network. Understanding these characteristics is important in evaluating the feasibility of the DSI

network to support Advanced Distributed Simulation (ADS) T&E efforts. The JADS ETE test is one such effort that is representative of that performed by T&E personnel. In this paper we examine the issues and the feasibility of running a JADS ETE test over the DSI. The issues can be broadly characterized as technical and managerial. The technical issues are: bandwidth, latency, and resource availability to run JADS ETE tests. The managerial issues are: costs, node locations, and exercise scheduling.

1.3 SCOPE

This report has a limited scope. It provides a short summary of the capabilities of the Phase II DSI. It gives simple examples, where appropriate, to provide the JADS community with a better feel for its features and capabilities. This report examines a JADS ETE test scenario that can be run over the DSI. Studying all the ETE test scenarios is beyond the scope of the present paper. Cost estimates are generally reliable; however, they should be confirmed to avoid surprises.

1.4 DOCUMENT ORGANIZATION

In Section 2, the DSI Phase II network is described in detail. Section 3 describes the JADS ETE test scenario and a possible DSI set up that could support the JADS test. Advantages and disadvantages of running JADS over DSI are presented. Section 4 presents the conclusions of this study. Appendixes present detailed information, such as, router configurations, and physical connectivity of VTC equipment.

Section 2

2. DSI PHASE II

The Phase II upgrade of the DSI was completed in October 1997. With this upgrade the DSI transitioned from proprietary products to standards-based products. In this section, the DSI topology and capabilities are discussed. These capabilities include: Resource ReSerVation Protocol (RSVP), multicasting, routing, video-teleconferencing (VTC), security, and network management. DSI membership information and future upgrade plans are discussed towards the end.

2.1 TOPOLOGY

The DSI backbone has seven nodes arranged in a partial mesh topology (Figure 1). Each node consists of a Cisco 7500 router connected to a Defense Information Systems Network (DISN) ATM Switch (not shown). Each of these switches, in turn, is connected to a commercial ATM cloud which provides 3 Megabits per second (Mbps) permanent virtual circuit (PVC) pipes among the nodes.

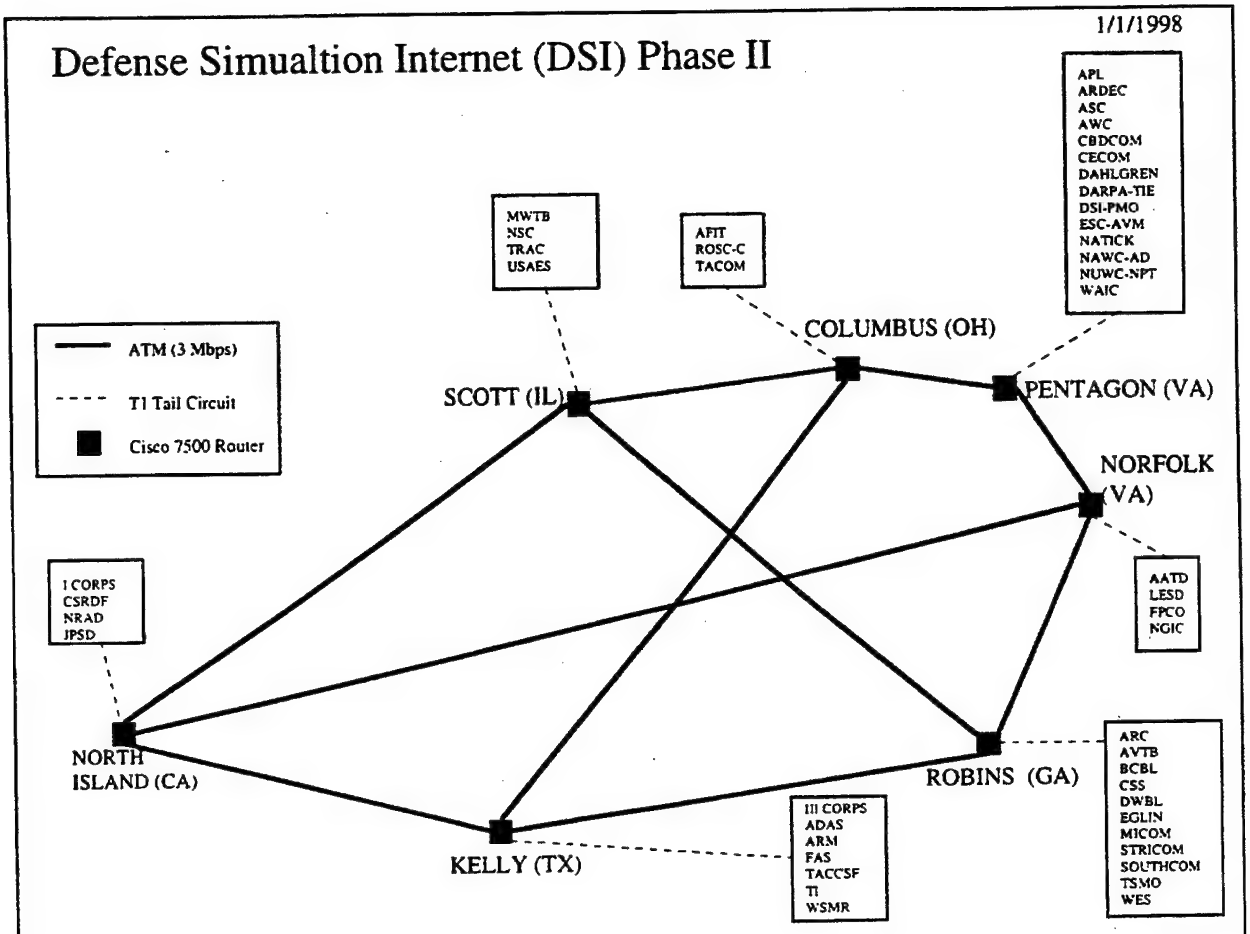


Figure 1. DSI Phase II Topology

The IP address assignments and the ATM connection identifiers such as Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) of the backbone ATM interfaces are shown in Figure 2.

Back Bone Node	IP Address / Mask 199.57.64.X / 30	Interface	Description	VPI, VCI
COLUMBUS	98	ATM0/0.1	To PENTAGON	0, 103
COLUMBUS	85	ATM0/0.2	To KELLY	4, 121
COLUMBUS	89	ATM0/0.3	To SCOTT	10, 120
KELLY	117	ATM0/0.1	To NORTH ISLAND	37, 122
KELLY	114	ATM0/0.2	To ROBINS	41, 126
KELLY	86	ATM0/0.3	To COLUMBUS	4, 121
NORFOLK	94	ATM0/0.1	To PENTAGON	0, 101
NORFOLK	101	ATM0/0.2	To ROBINS	49, 127
NORFOLK	105	ATM0/0.3	To NORTH ISLAND	0, 101
NORTH ISLAND	118	ATM0/0.1	To KELLY	37, 122
NORTH ISLAND	106	ATM0/0.2	To NORFOLK	39, 125
NORTH ISLAND	121	ATM0/0.3	To SCOTT	6, 124
PENTAGON	93	ATM0/0.1	To NORFOLK	0, 101
PENTAGON	97	ATM0/0.2	To COLUMBUS	0, 103
ROBINS	109	ATM0/0.1	To SCOTT	5, 123
ROBINS	113	ATM0/0.2	To KELLY	41, 126
ROBINS	102	ATM0/0.3	To NORFOLK	43, 127
SCOTT	110	ATM0/0.1	To ROBINS	5, 123
SCOTT	122	ATM0/0.2	To NORTH ISLAND	6, 124

Figure 2. IP Address Assignments of ATM Interfaces

Each backbone node is connected to several site nodes. There are a total of 46 tail sites at the present time. Each site node has a Cisco 7204 router with a serial T1 (1.54 Mbps) link to its backbone node. As an example, the configuration of one site (the Joint Precision Strike Demonstration (JPSD) site at Fort Huachuca, Arizona) is shown in Figure 3. We will also describe this configuration below.

Typically, a site router has one serial port and four Ethernet ports. One Ethernet interface is assigned a class C Internet Protocol (IP) address range for unclassified simulations. A single host IP address is available for desktop VTC (DVTC) via a second Ethernet interface. A third Ethernet segment connects to a port of the Improved Network Encryption System (INES) box built by the Motorola Corporation. This box helps in providing secure simulations and secure DVTC. Again, there is a complete class C IP address range for secure simulations and a single IP host address for secure DVTC. The simulation Local Area Network (LAN) and the DVTC LAN are connected to two Ethernet ports of a Cisco 4500 router on the red side (classified side). The maximum throughput from the INES is about 1.2 Mbps in both directions (combined) and is achieved by sending large packets (1400 Byte packets) through the INES. For smaller packets, the throughput is much smaller. To overcome this limitation, an aggregator box (which is a Personal Computer (PC) with a Pentium processor running on Free Berkeley System Distribution (BSD) operating system) connects to a third Ethernet interface of the Cisco 4500 router and an INES port (see Figure 3). Multicast traffic from the red side is packaged by the aggregator into larger packets and is shipped to the network via its black site router. Similarly multicast traffic destined for the red side is deaggregated and forwarded to the simulation LAN.

JPSD

FT. HUACHUCA, AZ

MODIFICATION DATE
25 SEP 97

EFFECTIVE DATE
25 SEP 97

Dial-In Phone:
Ckt ID:

POC#1 Robert A. Olson
Phone: 520-533-4612
FAX: 520-533-4605
Email:rob@huachuca-simcenter.army.mil

POC #2:
Ph#

Logistics:
Ph#

Property Book Officer:
Ph#

COMSEC SHIPPING ADDRESS:

SHIPPING ADDRESS:

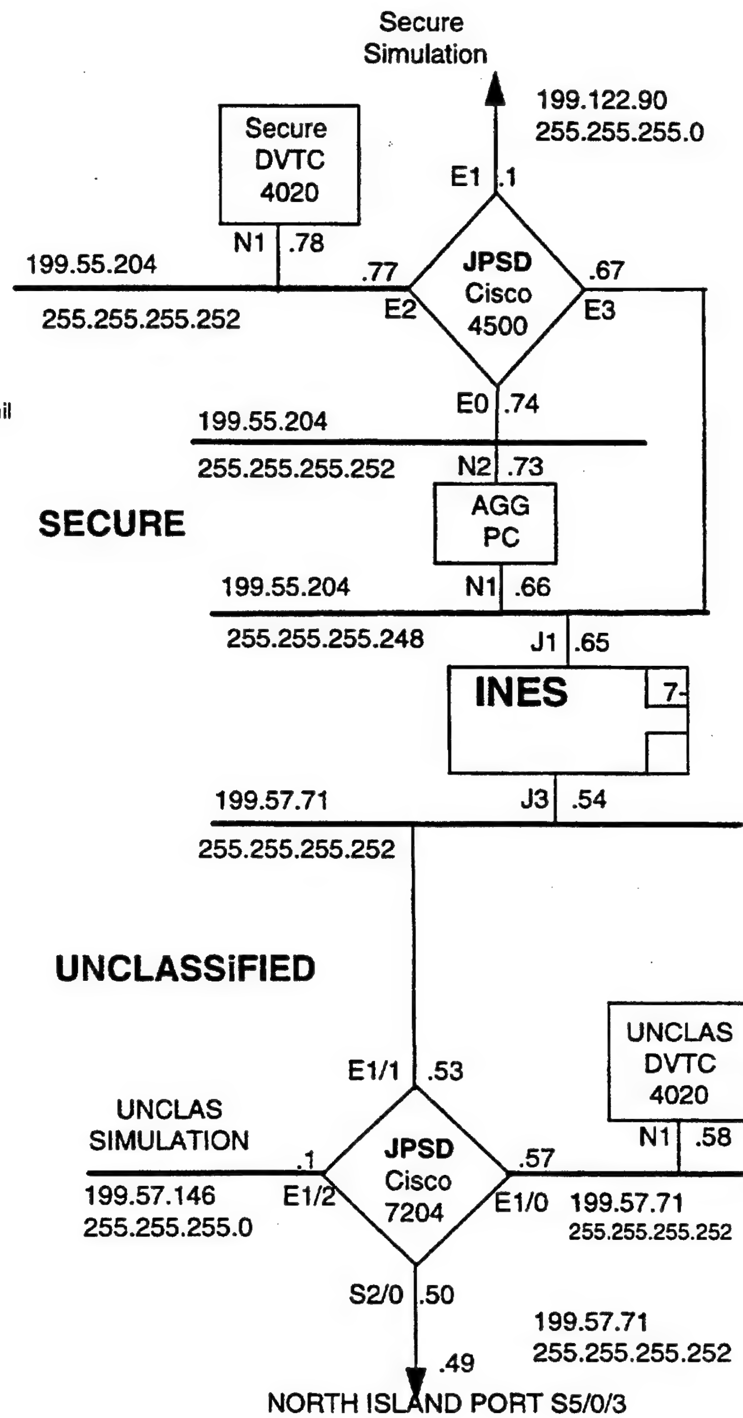


Figure 3. DSI Site Configuration

2.2 CAPABILITIES

The DSI phase II network supports standards-based protocols such as RSVP and H.320 VTC. In addition, the DSI network supports IP multicasting, link-state routing, secure and non-secure distributed simulations, and the usual internet and intranet applications such as file transfer, e-mail, telnet, and web-browsing. We highlight the main capabilities in the following subsections.

2.2.1 RSVP

The RSVP protocol reserves bandwidth for traffic moving from a source to a destination. Without RSVP, all traffic is treated on a best-effort basis. If the network is over-loaded, then packets in the traffic are dropped. With the invocation of RSVP, mission critical traffic is not dropped.

Request for Comment 2205 (RFC 2205) published by the Internet Engineering Task Force (IETF) lays down the functional specifications of RSVP. It states, "RSVP provides receiver-initiated setup of resource reservation for multicast or unicast data flows, with good scaling and robustness properties." The basic model of RSVP includes a sender application, that generates data, and a receiver application (or multiple receiver applications), that wishes to receive data. The sender transmits path messages downstream toward the receiver. This message is used to inform intermediate routers and the receiver (or group of receivers) about the characteristics of the path (such as bandwidth, delay, etc.) to be setup between the sender and the receiver. Based on this information, the receiver makes a reservation request and passes it upstream through the intermediate routers toward the source. At each intermediate router, the request is passed to admission control and policy control. Admission control checks to see if the node has sufficient available resources to grant the requested Quality of Service (QOS), and policy control checks to see if the user has permission to make the reservations. Both checks must be positive to reserve the necessary resources.

For applications that are not RSVP-capable, Cisco edge routers can be manually configured to install a reservation from a sender to a receiver. In order to successfully install a reservation through the network, all the intermediate routers must allocate RSVP bandwidths. If a link in the reservation chain is accidentally broken, then the reservation can be dynamically re-established via an alternate path, if resources along that path are available.

Some practical examples of making reservations in the DSI network are shown below.

- To setup a unicast reservation of 150 Kbps between a sender router A (IP address 199.57.127.10 and Ethernet interface Eth1/1) and a receiver router B (IP address 199.57.127.22 and Ethernet interface Eth2/1) the following configurations are entered in the routers.

  Router A (interface Ethernet1/1):

ip rsvp sender 199.57.127.22 199.57.127.10 UDP 0 0 199.57.127.10 Eth1/1 150 60

This statement sets up a path message from router A to router B using the user datagram protocol (UDP) with unassigned destination and source port numbers (0 0). A bandwidth of 150 Kbps is reserved for data flowing from the sender to the receiver with minimum burst size not exceeding 60 Kbps.

Router B (interface Ethernet2/1):

ip rsvp reservation 199.57.127.22 199.57.127.10 UDP 0 0 199.57.127.22 Eth2/1 ff load 150 60

This statement sets up a reservation message from the receiver to the source. The sender command on router A and the reservation command on router B jointly install a 150 Kbps reservation from A to B. This reservation is a fixed filter *(ff)* type implying that there is a single sender.

- To setup a native multicast reservation to the group 224.1.2.3 consisting of routers A (IP address 199.57.127.10 and Ethernet interface Eth1/1), B (IP address 199.57.127.22 and Ethernet interface Eth2/1), and C (IP address 199.57.125.15 and Ethernet interface Eth2/0), the following configurations are entered in the routers.

Router A (interface Ethernet1/1):

ip rsvp sender 224.1.2.3 199.57.127.10 UDP 0 0 199.57.127.10 Eth1/1 250 60

ip rsvp reservation 224.1.2.3 0.0.0.0 UDP 0 0 199.57.127.10 Eth1/1 wf load 500 60

The first statement sets up a path message from router A to the multicast group 224.1.2.3 using the UDP protocol with unassigned destination and source port numbers (0 0) with bandwidth 250 Kbps and the maximum burst size of the data not exceeding 60 Kbps. The second statement means that reservation messages from receivers in the multicast group come from all senders (address 0.0.0.0) and that the wild card filter (wf) reservation style applies.

Router B (interface Ethernet2/1):

ip rsvp sender 224.1.2.3 199.57.127.22 UDP 0 0 199.57.127.22 Et21/1 250 60

ip rsvp reservation 224.1.2.3 0.0.0.0 UDP 0 0 199.57.127.22 Eth2/1 wf load 500 60

The first statement sets up a reservation message from router B to router A. This reservation is a fixed filter *(ff)*.

Router C (interface Ethernet2/0):

ip rsvp sender 224.1.2.3 199.57.125.15 UDP 0 0 199.57.125.15 Eth1/1 250 60

ip rsvp reservation 224.1.2.3 0.0.0.0 UDP 0 0 199.57.125.15 Eth1/1 wf load 500 60

In addition, the statement *ip igmp join-group 224.1.2.3* should be inserted in the serial network interface of each of the routers A, B, and C.

2.2.2 Multicasting

Multicasting allows users to be members of a group of users and exchange traffic among themselves in an efficient manner. Membership in the group is activated through the Internet Group Management Protocol (IGMP). In addition, a routing protocol is needed to route traffic among its members. In the DSI, the protocol independent multicasting (PIM) dense-mode is used as the multicast routing protocol.

There are two modes of operations for multicast traffic. These two multicasting modes provide the DSI users with advanced features to run their applications among the participants in a test event. The first is a native multicasting, where an IP address range of 224.x.x.x to 254.x.x.x (where each x can be any number from 1 to 254) is used to indicate membership in the group. In native multicasting, packets are sent directly from a sender to a group of receivers. An example of reserving bandwidth for native multicasting was presented in the previous subsection. The DSI supports native multicasting applications such as VAT, which is an audio conferencing tool, and VIC, which is a video teleconferencing tool, and WB (white board), which is a chalk-board writing tool, all developed at the Lawrence Berkeley Laboratory. In addition, UDP traffic can be exchanged among members in the DSI. If the links, over which such UDP traffic is transmitted are congested, then packets could be dropped. However, if bandwidth is reserved for multicast flows, the UDP traffic will be protected.

The second mode of multicasting supported in the DSI is multicasting via subnet-directed broadcasting. This mode is useful for hosts that talk to each other by broadcasting a protocol data unit (PDU) to their local Ethernet. One such application is ModSAF (Modular Semi-automated Forces) which generates simulation entities and floods its local Ethernet with simulation PDUs. These entities then interact with entities generated by other hosts that participate in the distributed simulation exercise. The Cisco routers support a broadcast-to-multicast (and multicast-to-broadcast) functionality that allows routers to forward LAN traffic with time-to-live *(ttl)* scope of more than one router hop. An example of this "subnet-directed multicasting" configuration is given below, to give the readers a flavor of this advanced feature.

- Let the router A's Ethernet interface Eth1/1 (IP address 199.57.127.10) be connected to the LAN segment to which the ModSAF host is also attached (IP address 199.57.127.11). Let the serial interface S1/0 of router A be connected to the network.

Then the following statements are needed:

(interface Eth1/1)

ip multicast helper-map broadcast 224.1.2.3 100 ttl 10

(interface S1/0)

ip multicast helper-map 224.1.2.3 199.57.127.255 100

The first statement takes broadcast packets and forwards them to the group address 224.1.2.3 with access list of 100 and *ttl* of 10. The second statement accepts packets from the group 224.1.2.3 and broadcasts them to the Ethernet LAN to which the ModSAF host is attached.

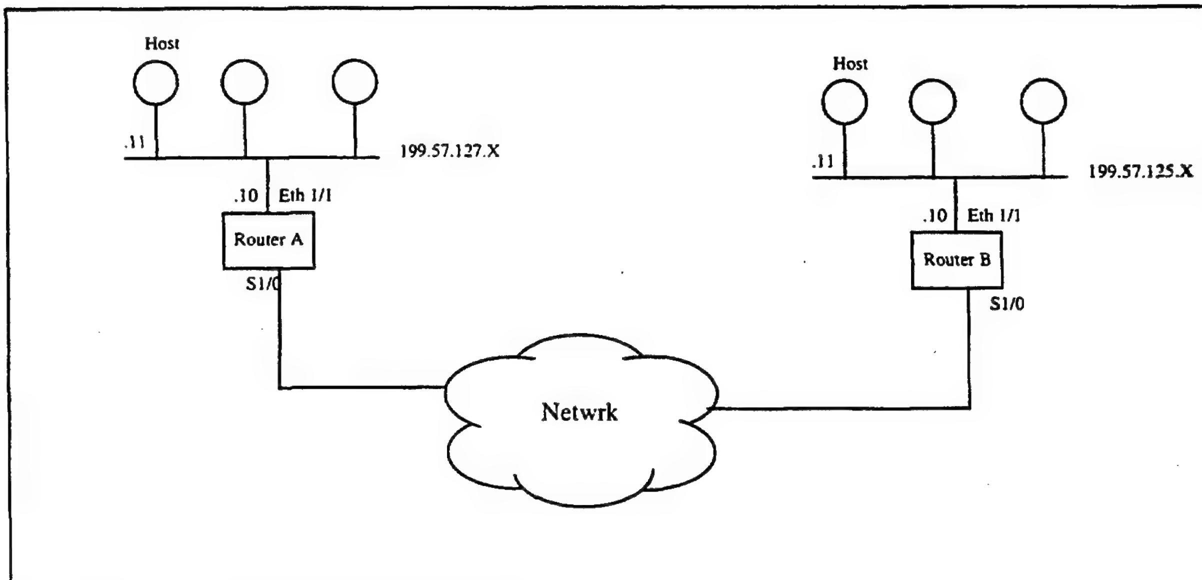


Figure 4. Configuration For Subnet-directed Broadcasting

2.2.3 Routing

The link-state protocol Open Shortest Path First (OSPF) is used for routing table updates within the DSI network. The network is partitioned into eight areas (area 0 through area 7). The backbone area is designated as area 0 with network address 199.57.64.0 and mask 255.255.255.0. The site areas are designated as area 1 through area 7 and share routing advertisements with the backbone area 0. Appendix A shows the OSPF configuration for the Norfolk backbone node, which belongs to area 2. The OSPF configuration for the Cisco 7204 site router at JPSD, which is linked to the North Island node and is part of area 7, is shown in Appendix B.

The Norfolk backbone router has an Ethernet link to the DISA Joint Information Services (JIS) router, which has connectivity to the Internet. The JIS router runs Cisco's proprietary Inter-gateway Routing Protocol (IGRP) and Enhanced-IGRP (EIGRP) in its routing domain. The IGRP autonomous system number is 568 for the JIS router. The DSI Norfolk router and the JIS router share routing updates via the Border Gateway Protocol 4 (BGP4) protocol. As shown in the BGP configuration in Appendix A, all the BGP advertisements for the entire DSI network are compactly done through the use of Classless Inter Domain Routing (CIDR) address blocks, beginning at 199.57.64.0 and 199.57.128.0 with their associated masks.

The routing for secure simulations and DVTC is done via default routing and a typical red Cisco 4500 configuration is shown in Appendix C. Further discussions of security aspects will be done in the security subsection.

The routing protocols in the DSI network are robust and have been thoroughly tested to prevent route-flapping and looping. OSPF and BGP provide state-of-art routing in the DSI network

2.2.4 VTC

DSI provides DVTC service among user sites with a maximum of four participants per session. The VTC equipment at a site consists of an Intel Pentium Personal Computer (PC) running the Windows 95 operating system installed on a removable hard drive. There are two identical removable hard drives of capacity one Gigabyte each. One hard drive is used for unclassified (black) VTC and the other for classified (red) VTC. A monitor, a pair of stereo speakers, and a camera are also included. The software for VTC and video-sharing are provided by Zydacron and PictureTel and integrated by Summit Solutions. The H.320 series of standards are used. These standards lay down the rules to transmit video/voice/data over Integrated Services Digital Network (ISDN) lines. Summit Solutions has developed a solution to convert the ISDN packets into Ethernet frames and then forward them to their destination. The frames can be transmitted at 64 Kbps through 384 Kbps in increments of 32 Kbps. There is an overhead of about 100 Kbps per frame, regardless of its payload. The emerging H.323 standards are expected to provide true packetized video over IP.

Point-to-point DVTC between any two video-equipped sites can be initiated. This is done by configuring the host IP address and the gateway IP address on the PC and by dialing a phone number in the database. White board, chat sessions, picture and file sharing can be invoked by the participants. For multiple participants in the VTC, RadVision's Gateway and Multipoint Control Unit (MCU) video-server units are needed. The MCU allows sessions among four participants and may be initiated by the Network Control Center (NCC) at Columbus, Ohio, where the MCU and the Gateway are configured. The MCU has four ports which connect to four ports of the Gateway which also has four Ethernet ports. These Ethernet ports are connected to four Ethernet ports on the Columbus backbone router (see

Appendix D). The participants request a conference ahead of time so that appropriate bandwidth may be reserved on the network for a successful video session.

The DVTC equipment is not only economical compared to bulky room system video that it replaced, but also provides additional savings by using the same equipment for both classified and unclassified work (except for the removable hard drive).

2.2.5 Security

Secure simulations and secure VTC may be done from the red side of a DSI site. The secure equipment consists of a Cisco 4500 router, a PC aggregator, VTC equipment, and an Improved Network Encryption System (INES) box manufactured by the Motorola Corporation. The INES provides DSI with end-to-end encryption. All the INES devices are administrated by an INES Enhanced Product Server (EPS) that does the following: configuration management, auditing, and electronic key management.

The INES is endorsed by the National Security Agency (NSA) to handle classified data up to the TOP SECRET level. However, for the DSI, it is authorized to handle only SECRET information. The INES provides for data confidentiality, data integrity, peer identification, and access control on the DSI. The INES has an unclassified LAN interface port (J3) that is connected to the unclassified network (black side). It has a classified LAN interface port (J1) that is connected to the classified network (red side). A key-shaped plastic case called KSD-64A (Key Storage Device) is used to store the following: a non-forgeable certificate, INES security platform identity, security classification, and an ASCII (American Standard Code for Information Interchange) identity. In addition to KSD-64A, a configuration floppy disk is needed to make the INES operational. At start up time the INES reads data on KSD-64A and stores it in non-volatile read-only memory (NVROM). The INES erases the KSD-64A, then creates and writes a Crypto Ignition Key (CIK) to it. The INES also calculates a cryptographic checksum for each file on the floppy disk. The INES writes a file called VERIFY.REC, that contains the checksum, to the floppy disk. In order to operate, the INES must have all the three parts mentioned above: the key data in NVROM, the CIK on KSD-64A, and the VERIFY.REC file on the floppy.

The INES takes packets forwarded to its red interface, encrypts the data, appends an IP header for transport across a black IP network, and ships them to the next-hop router. When an INES receives an encrypted packet, it decodes the packet and forwards to the red interface. For unicast sessions between a pair of INESs, a session key is established via a negotiation process between the pair. The INES maintains a table of session keys. For a multicast session, a multicast session key is established. As mentioned in section 2.1, the PC aggregator provides for better throughput for multicast traffic. The multicast traffic is forced to travel through the aggregator box via default route statements in the Cisco 4500 router, whereas the unicast traffic is default-routed to avoid the PC aggregator. A typical router configuration on the red side is given in Appendix C. Because of data encryption on the red

side, bandwidth reservation is not feasible. However, the traffic on the black side (unclassified side) can be reserved by invoking RSVP.

Multiway DVTC on the red side is scheduled with the help of 4 INESs, a Radvision Gateway, and a MCU at the Columbus backbone node. The black sides of the INESs are interfaced with 4 Ethernet ports on the Columbus backbone router.

2.2.6 Network Management

Network management functions are performed at the Network Control Center (NCC) at Columbus. Network controllers monitor backbone and site routers and circuits. They also provide help desk and trouble-shooting service, and set up exercises that are scheduled. The toll-free support number for the NCC at Columbus is 1-888-281-3286. The controllers use Hewlett-Packard Openview software (version 4.1.1) on a Solaris platform, in the black side, to assist them in monitoring faults and generating alarms. The current controllers, their phone numbers, and e-mail addresses are given in Appendix E:

In addition to the commercial tool mentioned above, a set of automated tools have been developed for the DSI. A user can use these tools to view incoming and outgoing traffic statistics at the site router. Authorized users can use the friendly interface provided by the tools to make unicast and multicast bandwidth reservations, configure router interfaces, view IP address assignments of all the routers, and view the up-down status of router interfaces. The tools also enable the controllers to reload all the router configurations automatically at a specific date and time and check for duplicate address assignments.

2.3 DSI MEMBERSHIP

Membership in the DSI community may be requested from DISA. The point of contact is Mr. T. Shannon at 703-735-8064 whose e-mail address is shannont@ncr.disa.mil. Another point of contact is Ms. Alice Bontrager at Columbus at 614-692-9138 whose e-mail address is bontragera@crcc.disa.mil. There is also a group e-mail address, dsicell@crcc.disa.mil that may be contacted for membership. Approximate cost for joining the DSI as a site node (at the time this report was written) is about *$60K* for equipment and about *$9K* per month for a T1 circuit charge. One Cisco 7204 router, one Cisco 4500 router, one INES, one PC aggregator, and one DVTC box with monitor and accessories are provided by DISA. The site is attached by a T1 tail circuit to one of the 7 backbone nodes. The backbone provides ATM PVC pipes of 3 Mbps among the 7 nodes in a partial mesh topology, as already mentioned.

2.4 FUTURE PLANS

Future upgrade plans for the DSI network include acquiring New INESs from the Motorola Corporation to increase throughput and decrease latency. H.323 compliant DVTC products and hardware-based codecs might also be acquired when they become available.

Section 3

3. JADS

In the previous section, we presented the characteristics, capabilities, and accessing information of the modernized DSI. The JADS Test force is interested in finding out if they can be part of this network and run their simulations. If this is feasible, then the T&E community can access DSI nodes and DSI simulation systems.

In this section we discuss a JADS ETE test configuration for T&E, a potential configuration for running this test over the DSI, and an evaluation of the DSI's suitability to support this test.

3.1 ETE TEST CONFIGURATION

The JADS ETE test consists of four phases. Phase 1 is a developmental phase in the laboratory that develops and integrates hardware and software for the test. Phase 2 is a phase (also in the laboratory) that tests the feasibility of ADS to support developmental T&E (DT&E) and operational T&E (OT&E). Phase 3 examines the interoperability of ADS with Joint Surveillance Target Attack Radar System (STARS) equipment. Finally phase 4 is a live test in which an actual airborne E-8C radar aircraft is linked to receivers and other systems on the ground.

In this report, the phase 2 test configuration is examined in detail. The network supporting this test scenario consists of five nodes: the Test, Control, and Analysis Center (TCAC) node located at Albuquerque, New Mexico; and four other nodes at: Fort Hood (III Corps), Texas; White Sands Missile Range (WSMR), White Sands, New Mexico; Grumman Aerospace Laboratory, Melbourne, Florida; and Fort Sill, Oklahoma. In this network, the TCAC is connected by dedicated T1 links to the other 4 nodes. In addition, the Joint STARS ground station at Grumman is connected to the ground station at Fort Hood by a simulated Surveillance and Control Data Link (SCDL) at a T1 rate. Test control among participating sites is done via one voice channel out of T1 link. A topology of the phase 2 ETE test scenario is shown in Figure 5.

1/1/1998

JADS End-to-End Test Phase 2 Topology

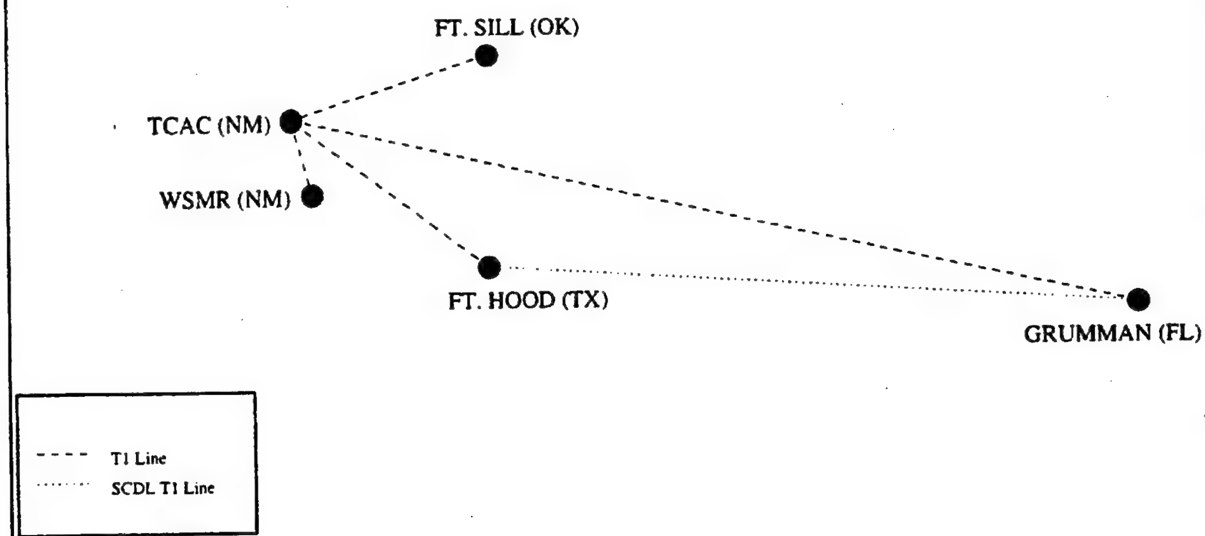


Figure 5. JADS Phase 2 ETE Test Topology

The network baseline requirements for running the JADS ETE phase 2 test on the DSI are derived from engineering analysis of expected data traffic. The derived requirements are (based partly on correspondence with JADS ETE Test Team Lead Lt. Col. Mark McCall):

1. The bandwidth (including voice) utilized in any given T1 link should not exceed that of 1/2 of a T1 link.
2. The aggregate bandwidth exceeded that of a T1 link but did not exceed that of a dual T1 link.
3. The upper limit of latency including allowable errors and radar timelines should be no longer than a second.

4. The exercises are classified.

3.2 JADS ETE TEST OVER DSI

A potential configuration for running a phase 2 ETE test over the DSI is shown in Figure 6.

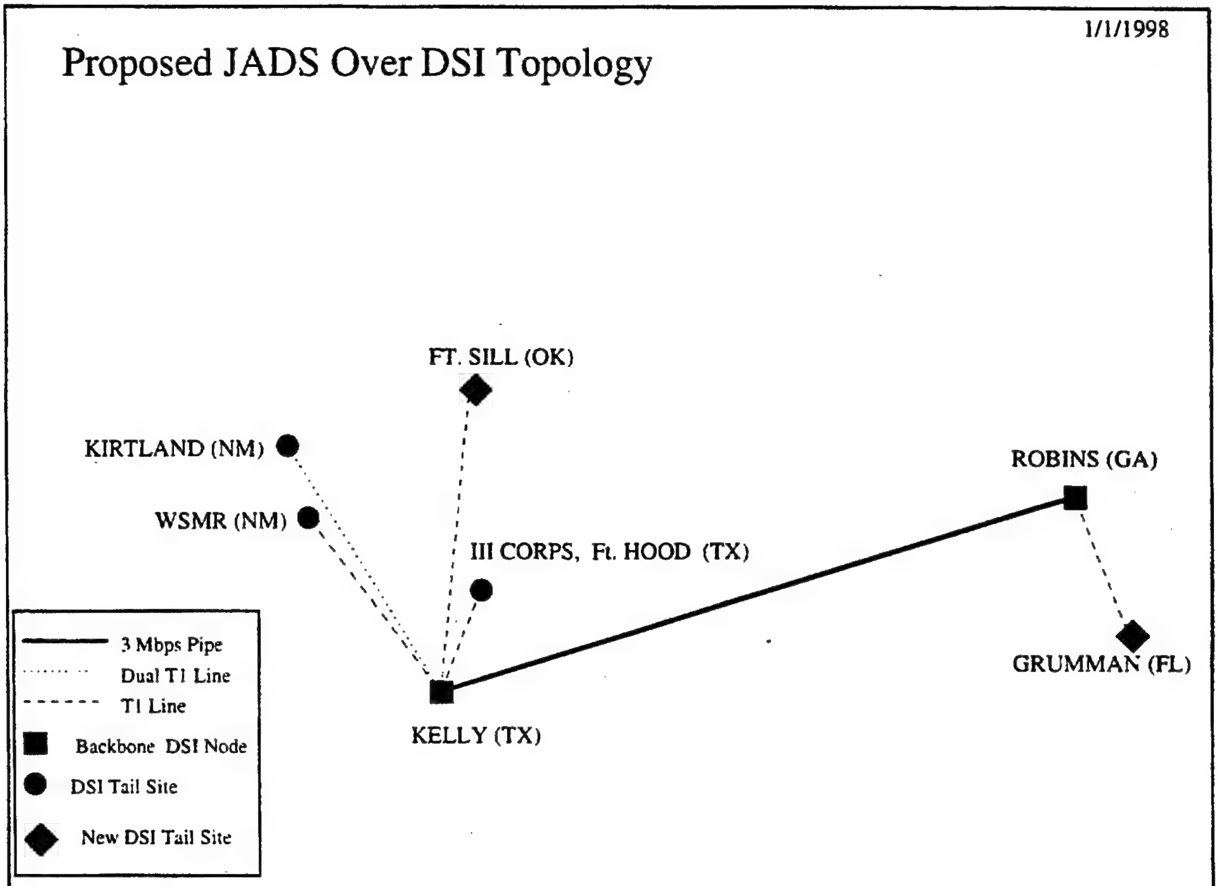


Figure 6. Proposed JADS ETE test over DSI Topology

The following assumptions have been made:

- The three existing DSI site nodes at WSMR, III Corps (Fort Hood), and KIRTLAND are available for JADS tests.
- Connectivity to two new DSI site nodes will exist. A new node at Fort Sill will be connected to the DSI backbone at KELLY. A new node at Grumman will be connected to the DSI backbone at ROBINS.

- The KIRTLAND node has a dual T1 link to KELLY. Inverse multiplexers are installed on the links between KELLY and KIRTLAND.
- Traffic in the backbone does not exceed 3 Mbps.
- The maximum latency in the backbone (measured by round-trip ping time) is 70 msecs. The maximum round-trip latency in the classified side (including INESs and aggregators) is assumed to be 100 msecs.
- Encryption is done by INESs. This is different from the KIV-7 encryption in JADS ETE tests.
- There exists a simulated SCDL link between the ground station at Grumman and the ground station at Fort Hood.

3.3 DSI SUPPORT OF JADS ETE PHASE 2 TESTS

Here we summarize the capabilities of the DSI and discuss the feasibility of the DSI to support JADS phase 2 ETE tests.

The DSI provides a robust network from which sites may be picked to participate in a JADS exercise. It provides a diverse community of sites to choose from. Standards based RSVP protocols on the DSI provide for bandwidth reservation. RSVP not only allows for latency bounds to be set up for packets, but also allows for efficient merging of reservations in a session. Bandwidth reservation is dynamic so that if a link goes down, traffic is automatically re-routed. Multicasting is supported so that packets in a distributed simulation are efficiently forwarded. Free internet tools such as VAT and VIC can be used for native multicasting among participating sites. Security is provided by INESs as discussed earlier. Network management tools allow for easy monitoring of the network.

JADS sites may be connected to the DSI to take advantage of the above features. However, there are costs associated with joining the DSI. These costs include equipment and monthly service charges. The equipment costs for two new sites is $120K. The circuit charges for the tail sites and the dual T1 line at KIRTLAND will be $27K per month. In addition the inverse multiplexers cost about $7K each. These costs may make running of JADS ETE test over the DSI uneconomical.

To run classified exercises, the limitations of the INESs need to be considered. The INES cannot match the link speed of a dedicated T1 link. The maximum throughput for large packets through the INES is about 1.2 Mbps in both directions.

Another serious problem arises if a site plans to continuously use the backbone links for an extended period of time and plans to run bandwidth intensive applications. With more than 50 sites and each backbone link having a capacity of 3 Mbps, a site may not be able to reserve

adequate bandwidth. Moreover, a site may not like the annoyance of scheduling and requesting bandwidth ahead of time.

To run video applications, the limitations of DVTC products should be considered. The DVTC products cannot be rated as excellent as far as performance is concerned. As mentioned earlier, there is considerable overhead in a DVTC session. This has an impact on performance, which JADS users may not be willing to accept.

Section 4

4. CONCLUSIONS

In this report we have presented a detailed review of the capabilities of modernized Phase II DSI. The topology of the DSI is presented. In addition, various capabilities of the DSI such as RSVP, multicasting, routing, VTC, security, and network management have been discussed. Information about the points of contact and the costs of joining the DSI have also been presented. Finally, possible future upgrade directions of the DSI have also been indicated. This information will be useful in making an informed decision on joining the DSI based on a particular group's requirements and budgets.

We also have considered a particular JADS ETE test scenario and the feasibility of running it over the DSI. A possible ETE test scenario over the DSI is presented. We listed the baseline requirements for running the JADS phase two ETE test on the DSI from what was observed in the actual test. We also discussed the feasibility of using DSI to support JADS phase two ETE test.

From a technical point of view, JADS ETE testing over the DSI is currently not a viable option. The main reason for this recommendation is the throughput limitations of the INES boxes. The two-way throughput for large packets (packet size of at least 1400 Bytes) is only 1200 Kilobits per second. From an economical point of view, the costs mentioned in the previous section may provide additional constraints for JADS to join the DSI. Finally, scheduling considerations may provide further annoyance for joining the DSI.

It is recommended that the issue of joining the DSI be revisited when DISA upgrades the INESs on the DSI to New INESs which are supposed to match the throughputs of T1 lines. At that time, there are no technical constraints expected for joining the DSI to link T&E simulations. The issue may be evaluated purely on an economic basis. It should be emphasized that the DSI provides robust standards-based state-of-the art IP protocols.

Appendix A

NORFOLK BACKBONE ROUTER CONFIGURATION

```
!
version 11.2
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname NORFOLK
!
boot system flash slot0:rsp-pv-mz.112-6
enable secret XXXXXXXXXXX
!
ip subnet-zero
ip host lesd 199.57.66.2
ip host nor 199.57.64.94
ip host kel 199.57.64.114
ip host sco 199.57.64.122
ip host fpco 199.57.66.26
ip host col 199.57.64.98
ip host rob 199.57.64.102
ip host pen 199.57.64.93
ip host nisl 199.57.64.106
ip host ngic 199.57.66.38
ip host aatd 199.57.66.14
ip domain-name les.mil
ip name-server 199.57.127.70
ip name-server 199.57.127.150
ip multicast-routing
ip dvmrp route-limit 7000
!
interface ATM0/0
 mtu 9180
 no ip address
 ip pim dense-mode
 no ip mroute-cache
 ip rsvp bandwidth 5000 5000
 no ip route-cache optimum
```

```
!
interface ATM0/0.1 point-to-point
 description ATM Link to PENTAGON
 ip address 199.57.64.94 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 2250 2250
 atm pvc 1 0 101 aal5snap
 traffic-shape rate 3000000 75000 75000
!
interface ATM0/0.2 point-to-point
 description ATM Link to Robins
 ip address 199.57.64.101 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 2250 2250
 atm pvc 2 43 127 aal5snap
 traffic-shape rate 3000000 75000 75000
!
interface ATM0/0.3 point-to-point
 description ATM Link to North Island
 ip address 199.57.64.105 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 2250 2250
 atm pvc 3 39 125 aal5snap
 traffic-shape rate 3000000 75000 75000
!
interface Serial1/0/0
 no ip address
 ip rsvp bandwidth 1382 1382
 shutdown
 fair-queue 64 256 23
!
interface Serial1/0/1
 description Link to GUNTER
 ip address 199.57.64.21 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial1/0/2
```

```
 description link to NGIC ccsd = 2820 ckt w36636/ds1-963441
 ip address 199.57.66.37 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial1/0/3
 description link to LESD ccsd = 28ef ckt uhc504
 ip address 199.57.66.1 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial4/0/0
 no ip address
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 shutdown
 fair-queue 64 256 1000
!
interface Serial4/0/1
 no ip address
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 shutdown
 fair-queue 64 256 1000
!
interface Serial4/0/2
 description link to AATD ccsd = 28q9 ckt 52hcga288710cv
 ip address 199.57.66.13 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial4/0/3
 description lint to FPCO ccsd = 282U ckt w36645
 ip address 199.57.66.25 255.255.255.252
```

```
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial4/1/0
 no ip address
 shutdown
!
interface Serial4/1/1
 no ip address
 shutdown
!
interface Serial4/1/2
 no ip address
 shutdown
!
interface Serial4/1/3
 no ip address
 shutdown
!
interface Serial5/0/0
 no ip address
 shutdown
!
interface Serial5/0/1
 no ip address
 shutdown
!
interface Serial5/0/2
 no ip address
 shutdown
!
interface Serial5/0/3
 no ip address
 shutdown
!
interface Serial5/1/0
 no ip address
 shutdown
```

```
!
interface Serial5/1/1
 no ip address
 shutdown
!
interface Serial5/1/2
 no ip address
 shutdown
!
interface Serial5/1/3
 no ip address
 shutdown
!
interface Ethernet6/0/0
 description Ethernet connection to JIS router
 ip address 198.26.132.42 255.255.255.252
 ip pim dense-mode
 load-interval 30
!
interface Ethernet6/0/1
 no ip address
 shutdown
!
interface Ethernet6/0/2
 no ip address
 shutdown
!
interface Ethernet6/0/3
 no ip address
 shutdown
!
router ospf 1
 redistribute bgp 3520
 network 199.57.64.20 0.0.0.3 area 0
 network 199.57.66.0 0.0.0.3 area 2
 network 199.57.65.108 0.0.0.3 area 2
 network 199.57.66.12 0.0.0.3 area 2
 network 199.57.64.92 0.0.0.3 area 0
 network 199.57.66.24 0.0.0.3 area 2
 network 199.57.64.104 0.0.0.3 area 0
```

```
network 199.57.64.100 0.0.0.3 area 0
network 199.57.64.24 0.0.0.3 area 0
network 199.57.66.36 0.0.0.3 area 2
default-information originate always
area 0 range 199.57.64.0 255.255.255.0
area 2 stub no-summary
area 2 default-cost 110
!
router bgp 3520
 no synchronization
 network 199.57.64.0 mask 255.255.192.0
 network 199.57.128.0 mask 255.255.192.0
 neighbor 198.26.132.41 remote-as 568
!
ip classless
ip route 0.0.0.0 0.0.0.0 198.26.132.41
ip route 199.57.64.0 255.255.192.0 Null0
ip route 199.57.128.0 255.255.192.0 Null0
!
snmp-server community public RO
snmp-server community private RW
!
line con 0
line aux 0
 modem InOut
 transport input telnet
 stopbits 1
 rxspeed 19200
 txspeed 19200
 flowcontrol hardware
line vty 0 4
 password 7 08315E4B0D18111800
 login
!
end
```

Appendix B

JPSD SITE ROUTER CONFIGURATION

```
!
version 11.2
service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname JPSD
!
boot system flash slot0:c7200-p-mz.112-6
enable secret XXXXXXXXXXXXXXX
enable password XXXXXXXX
!
ip subnet-zero
ip domain-name les.mil
ip name-server 199.57.127.70
ip name-server 199.57.127.150
ip multicast-routing
ip dvmrp route-limit 7000
!
interface Loopback0
 no ip address
 no ip mroute-cache
 no ip route-cache
 shutdown
!
interface Ethernet1/0
 description Link to DVTC
 ip address 199.57.71.57 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
!
interface Ethernet1/1
 description Link to INES J3
 ip address 199.57.71.53 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
```

```
!
interface Ethernet1/2
 description Link to Unclass Sim
 ip address 199.57.146.1 255.255.255.0
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
!
interface Ethernet1/3
 no ip address
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 shutdown
 fair-queue 64 256 1000
!
interface Serial2/0
 description link to N.ISLAND ccsd = 283k ckt mgs969320-151
 ip address 199.57.71.50 255.255.255.252
 ip pim dense-mode
 ip rsvp bandwidth 1382 1382
 bandwidth 1544
 fair-queue 64 256 1000
!
interface Serial2/1
 no ip address
!
interface Serial2/2
 no ip address
 shutdown
!
interface Serial2/3
 no ip address
 shutdown
!
router ospf 1
 passive-interface Ethernet1/0
 passive-interface Ethernet1/1
 passive-interface Ethernet1/2
 network 199.57.71.48 0.0.0.3 area 7
 network 199.57.71.52 0.0.0.3 area 7
 network 199.57.146.0 0.0.0.255 area 7
```

```
 network 199.57.71.56 0.0.0.3 area 7
 area 7 stub no-summary
!
ip classless
ip forward-protocol udp 3000
ip forward-protocol udp 3001
ip forward-protocol udp 3002
access-list 100 permit ip any any
!
snmp-server community public RO
!
line con 0
line aux 0
 modem InOut
 transport input telnet
 stopbits 1
 rxspeed 19200
 txspeed 19200
 flowcontrol hardware
line vty 0 4
 password 7 0314490E020E35435C
 login
!
end
```

Appendix C

JPSD RED ROUTER CONFIGURATION

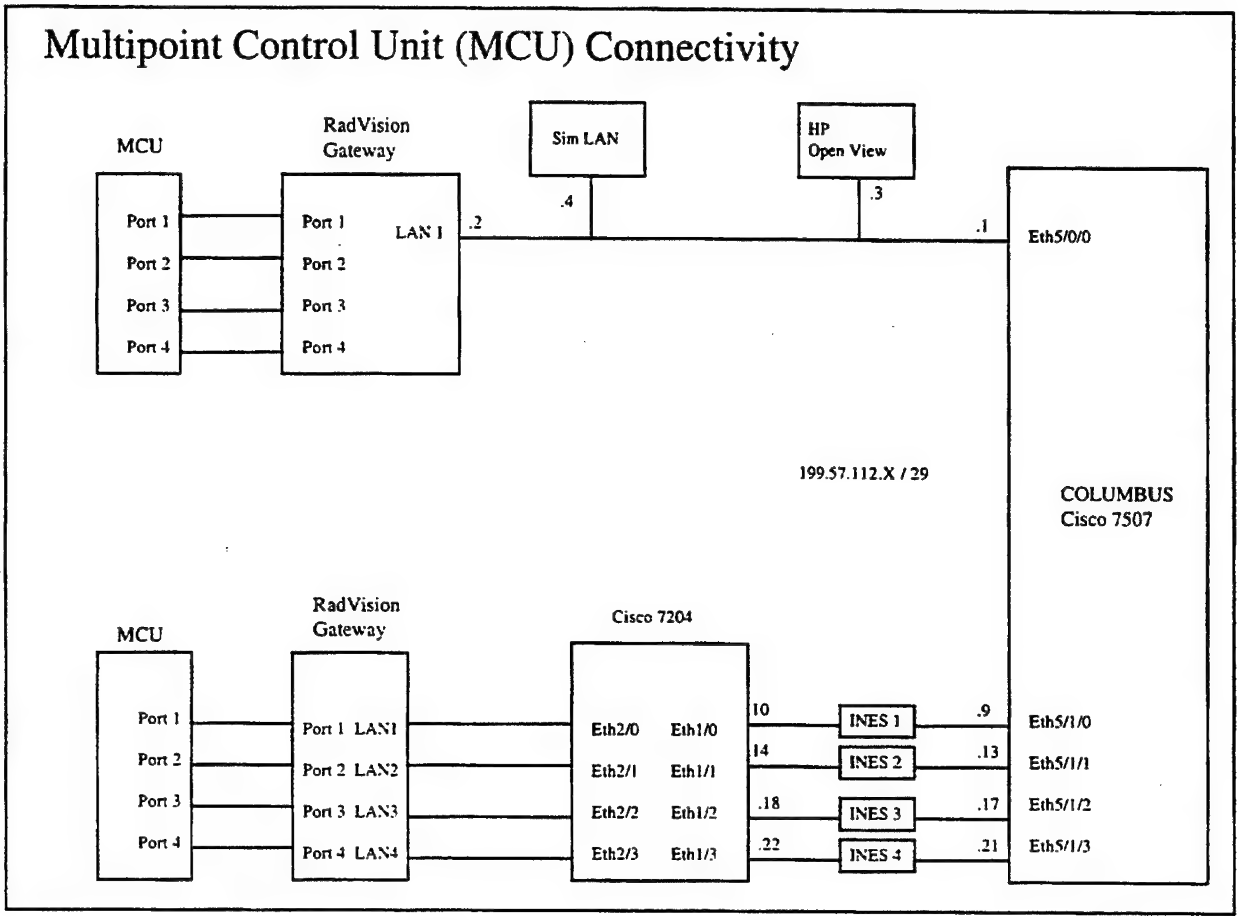
```
!
version 11.2
service udp-small-servers
service tcp-small-servers
!
hostname JPSD-4500
!
enable secret XXXXXXXXXXXXXXX
enable password xxxxx
!
ip subnet-zero
no ip domain-lookup
ip name-server 199.55.156.100
ip multicast-routing
ip dvmrp route-limit 7000
!
interface Ethernet0
 description Ethernet to Aggregator
 ip address 199.55.204.74 255.255.255.252
 ip pim dense-mode
 ip multicast helper-map 224.5.5.5 199.122.90.255 100
 ip igmp join-group 224.5.5.5
 media-type 10BaseT
!
interface Ethernet1
 description SIM-LAN
 ip address 199.122.90.1 255.255.255.0
 ip pim dense-mode
 ip multicast helper-map broadcast 224.5.5.5 100 ttl 10
 media-type 10BaseT
!
interface Ethernet2
 description DVTC-LAN
 ip address 199.55.204.77 255.255.255.252
 media-type 10BaseT
!
```

```
interface Ethernet3
 description Ethernet to INES
 ip address 199.55.204.67 255.255.255.248
 ip pim dense-mode
 load-interval 30
 media-type 10BaseT
!
interface Ethernet4
 no ip address
 shutdown
!
interface Ethernet5
 no ip address
 shutdown
!
ip classless
ip forward-protocol udp 4000
ip forward-protocol udp 4001
ip forward-protocol udp 3000
ip forward-protocol udp 3001
ip forward-protocol udp 3002
ip route 0.0.0.0 0.0.0.0 199.55.204.65
ip mroute 0.0.0.0 0.0.0.0 199.55.204.73
access-list 100 permit ip any any
tftp-server flash c4500-i-mz.112
!
line con 0
line aux 0
 transport input all

line vty 0 4
 exec-timeout 60 0
 password XXXXX
 login
!
end
```

Appendix D

COLUMBUS MCU



Appendix E

Columbus Control Center Personnel

Columbus Network Control Center Controller Information:

1. Mr. T. Brown, phone 614-692-6302, e-mail: tbrown@crcc.disa.mil
2. Mr. M. Boeck, phone 614-692-2223, e-mail: mboeck@crcc.disa.mil
3. Mr. J. Colley, phone 614-692-6320, e-mail: jcolley@crcc.disa.mil

Glossary

ADS	Advanced Distributed Simulation
ATM	Asynchronous Transfer Mode
ASCII	American Standard Code for Information Interchange
BBN	Bolt Beranek and Newman
BGP	Border Gateway Protocol
BSD	Berkeley System Distribution
CIDR	Classless Inter Domain Routing
CIK	Crypto Ignition Key
CN	Concentrator Node (a router product from Bay Networks)
DASU	DISN ATM Switch Unclassified
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DISN	Defense Information Systems Network
DSI	Defense Simulation Internet
DT&E	Developmental Test and Evaluation
DVTC	Desktop Video Teleconferencing
EIGRP	Enhanced IGRP (Cisco Systems Proprietary)
EPS	Enhanced Product Server
ETE	End-to-end
EW	Electronic Warfare
ff	Fixed Filter (a reservation style in RSVP)
HLA	High Level Architecture
IETF	Internet Engineering Task Force
IGMP	Internet Group Membership Protocol
IGRP	Inter-gateway Routing Protocol (Cisco Systems Proprietary)
INES	Improved Network Encryption System
IP	Internet Protocol
ISDN	Integrated Services Digital Network
JADS	Joint Advanced Distributed Simulation
JIS	Joint Information Services

JPSD	Joint Precision Strike Demonstration
JSTARS	Joint Surveillance Target Attack Radar System
Kbps	Kilobits per second
KSD	Key Storage Device
LAN	Local Area Network
LN	Link Node (
Mbps	Megabits per second
MCU	Multipoint Control Unit
ModSAF	Modular Semi-Automated Forces
NCC	Network Control Center
NSA	National Security Agency
NVROM	Non-volatile Read-Only Memory
OSD	Office of the Secretary of Defense
OSPF	Open Shortest Path First
OT&E	Operational Test and Evaluation
PC	Personal Computer
PIM	Protocol Independent Multicasting
PVC	Permanent Virtual Circuit
QOS	Quality of Service
RFC	Request for Comment
RSVP	Resource ReSerVation Protocol
SIT	Systems Integration Test
ST II	Streams Protocol, Version II
STAR	Surveillance Target Attack Radar System
T1	System that transports Digital Signal Level 1 (1.544 Mbps)
T&E	Test and Evaluation
TCAC	Test, Control, and Analysis Center
ttl	time to live
UDP	User Datagram Protocol

VAT	A Free Audio-conferencing Tool
VCI	Virtual Channel Identifier
VIC	A Free Video-conferencing Tool
VPI	Virtual Path Identifier
VTC	Video Teleconferencing
WB	White Board
wf	Wild-card filter (a reservation style in RSVP)
WSMR	White Sands Missile Range

Distribution List

Internal

W010

J. S. Quilty

W110

J. C. Slaybaugh

W150

H. J. Carpenter
R. Eftekari

W15D

J. S. Dahmann

W15E

C. E. Walters (5)
E. R. Gonzalez
G. A. Tsoucalas
F. R. Richards
M. Hammond
Files (2)

W15F

M. Adams
S. Chakravorty
D. Sahu (5)
N. Schult

W062

N. J. Slattery
S. Welman

Records Resources (3)

External

Office of the Under Secretary of Defense
(Acquisition)
Deputy Director, Test,, systems Engineering &
Evaluation/Systems Assessment
ATTN: Lt. Col. Steven Cameron
The Pentagon, Room 3D1080
Washington, DC 20301-3110 (5)

Colonel Mark Smith
JADS Joint Test Director
JADS JTF
11104 Menaul Blvd., NE
Albuquerque, NM 87112 (10)

Appendix D

Impact of ATM on JADS

WN 98W000033

MITRE REPORT

Impact of ATM on JADS

April 1998

Devaraj Sahu

MITRE

Washington C[3] Center
McLean, Virginia

Abstract

This report investigates the feasibility of an Asynchronous Transfer Mode (ATM) network to support Test and Evaluation (T&E) requirements such as the Joint Advanced Distributed Simulation (JADS) phase two end-to-end (ETE) test. It gives a broad overview of ATM and discusses how an ATM network could support JADS ETE T&E efforts.

This report reviews key concepts behind ATM such as service classes, quality of service, and available signaling types. Two methods of running Internet Protocols (IP) applications over ATM are discussed. These two methods are: classical IP over ATM and Local Area Network Emulation (LANE). Applications running ATM in the native mode are also discussed.

A JADS phase two ETE test configuration for T&E is discussed and a potential configuration for running this test over an ATM network is presented. Equipment costs and ATM service costs are given. Questions raised by the JADS T&E community are answered.

Table of Contents

Section 1

1. INTRODUCTION

The Joint Advanced Distribution System (JADS) program is chartered by the Office of the Secretary of Defense (OSD) to investigate the utility of Advanced Distributed Simulation (ADS) for Test and Evaluation (T&E) applications. JADS has also been asked to identify ADS constraints and methodologies when used for T&E and to identify requirements for ADS systems to better support T&E in the future.

The JADS Joint T&E project consists of three test programs: the System Integration Test (SIT), End-to-End (ETE) test, and finally Electronic Warfare (EW) test. The SIT test has been scheduled to run from 1995 through 1998 and the EW and ETE tests will run through 1999. For each phase of a given test program, there is an associated test scenario that defines a prescribed set of interactions among the program entities. For JADS T&E efforts, a key element of the test program is the communications infrastructure that supports the execution of a test scenario.

In anticipation of extending the application of Asynchronous Transfer Mode (ATM) technology to support simulation applications for T&E, the JADS Test Director requested that MITRE review the status of ATM technology and its capability to support T&E requirements such as those represented by SIT, ETE, and EW tests. In response, MITRE's Network and Communications Engineering Center initiated a study to address the impact of ATM technology for distributed simulation based T&E. This paper looks at one phase of the JADS ETE test program and discusses how ATM could be used to support this test and what impact it could have from a cost and performance perspective.

1.1 BACKGROUND

ATM technology is gaining acceptance in both private and government communications networks. There are three main reasons for this increased acceptance. First, the equipment vendors are making standards-compliant products that are interoperable. Second, as the ATM technology matures, prices are steadily coming down. Finally, the availability of high-bandwidth pipes supporting traffic with different Quality of Service (QoS) requirements for transport of ATM traffic makes ATM a well-liked candidate in the wide area network (WAN). The T&E community is becoming aware of the acceptance of ATM technology and wants to find out what impact ATM will have on distributed simulation.

1.2 PURPOSE

This paper has three purposes. The first purpose is to identify and document aspects of ATM that may be of interest to the T&E community for T&E applications. The second

purpose is to examine the use of ATM to support a distributed simulation exercise. The final purpose is to provide answers to issues of concern to the T&E community about ATM networks. Since cost is a real concern in fielding any network, approximate cost estimates of equipment and services are given. It is hoped that this paper will provide personnel in the T&E community information that helps them in the application of this complex technology.

1.3 SCOPE

This paper provides a high-level review of ATM. Additional and more comprehensive information about ATM can be found in the reference section.

In this paper, we examine a representative JADS ETE test that can be run over an ATM network. An evaluation of all JADS tests is beyond the scope of this paper. Finally, the cost estimates given in this paper are meant to be guidelines only and are not firm quotes. More importantly, these cost estimates will change over time.

A list of JADS ATM questions addressed by this paper follows:

- Would the ATM network be public or private? If public, what impact would other traffic have on latency of JADS data?
- What are the encryption issues? How can encryption be accomplished between sites? Would we have to invest in NES rather than KIV-7?
- What is the impact on bandwidth?
- What is the impact on latency? Will latency be fixed or variable?
- Will small packet size require more processing at simulation sites? Will this add variable latency equal to or greater than WAN savings?
- Will multicast be easier or harder with ATM?
- Will ATM be more or less reliable?
- What are cost implications? Will T1 costs go up? Will new boxes be needed at simulation sites?
- What would it take for us to build our own private ATM network (i.e. cost, equipment, training, etc.)?

1.4 DOCUMENT ORGANIZATION

Section 2 gives a broad overview of ATM. Many of the key concepts behind ATM such as service classes, quality of service, and signaling are discussed. Several options for running Internet Protocol (IP) traffic in an ATM network are also discussed. Work on running applications directly over ATM, referred to as "native mode" ATM is also discussed.

Section 3 presents a JADS ETE test scenario that can be run over an ATM network. Answers to issues of concern to the JADS T&E community are also discussed, and a cost analysis of equipment and services is given. Finally conclusions are presented in Section 4.

Section 2

2. ATM

In this section we highlight some aspects of ATM believed to be important to the T&E community. We first present a general overview of ATM. Next we discuss issues concerning IP and ATM. Finally, we discuss native ATM services.

2.1 ATM OVERVIEW

The ATM specifications are formulated by the International Telecommunications Union (ITU) and the ATM Forum. The ITU is a United Nations special agency responsible for formulating telecommunications standards. The ATM Forum is an international non-profit organization formed with the objective of accelerating the use of ATM (Asynchronous Transfer Mode) products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness [for more information see their web page: www.atmforum.com]:

The ATM Forum has three types of members: Principal, Auditing, and Passive. A Principal member is an active member of the Forum and pays $10,000 annually towards membership. The Auditing and User membership are both passive with annual membership dues of $2,000 and $1,500 respectively. The Forum has a Technical Committee which has five meetings a year, each lasting a week. Only Principal Members may contribute papers for the working group specifications. There are twelve working groups in the Technical Committee. These working groups are: Control Signaling, LAN Emulation/Multiprotocol, Network Management, Physical Layer, Residential Broadband, Routing Addressing, Security, Service Aspects and Applications, Testing, Traffic Management, Voice and Telephony over ATM, and Wireless ATM.

The ATM Forum has been instrumental in developing and documenting specifications for ATM internetworking and promoting interoperability among vendor equipment. It also writes extensions to the ITU standards. In the following, we explain some of the key concepts behind ATM.

2.1.1 What is ATM?

ATM is a packet-switching technology that uses fixed-length packets called cells. Each cell is 53 octets long with a 5 octet header and a 48 octet payload. The payload can contain voice, data, or video information. In fact, these three kinds of traffic can be carried on the ATM network at the same time.

The asynchronous in ATM means that the cells originating from different traffic sources are *statistically multiplexed* as they arrive at an ingress ATM device such as a switch. At the

receiver end the cells are demultiplexed in the exact order they arrive at the egress switch. There is no resequencing of cells because they do not arrive out of order. The asynchronous nature of ATM traffic should be contrasted with synchronous traffic such as Digital Signal Level 3 (DS3 with a capacity of 44.74 megabits per second (Mbps)) transport which uses Time Division Multiplexing (TDM). In a synchronous transfer mode, TDM slots are synchronously transferred, whether there is traffic or not, thus wasting bandwidth. In contrast, ATM does not reserve slots for a pre-assigned traffic stream.

The logical ATM connections of a cell are determined by the Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI) fields in a cell header. The VPI/VCI combination is meaningful in the context of a given interface. The communication channels that transport ATM cells are called Virtual Connections. There are two types of virtual connections: Virtual Path Connection (VPC) and Virtual Channel Connection (VCC). A VPC is a collection of VCCs. A VCC is identified by a set of VPI/VCI values between two end points of the network. Connections can be established manually (Permanent Virtual Circuit (PVC)) or dynamically (Switched Virtual Circuits (SVC)). As the name implies, PVCs remain established permanently. In a PVC scenario, both point-to-point and point-to-multipoint connections can be established. SVCs are set up on a need-only basis using the signaling protocols of the ATM Forum. The duration of SVCs varies depending on the needs of the application. SVC makes manual setting up of connections unnecessary.

2.1.2 Why ATM?

The use of packet-switching by ATM is advantageous for several reasons. Cell-switching (a cell being a short packet) can handle both delay-sensitive traffic (such as voice and video) and loss-sensitive traffic (such as data) all at the same time. Multiple traffic streams with different traffic characteristics can share the same physical path in the network. Furthermore, ATM provides a range of high-speeds- from a few Mbps up to 10 Gigabits per second (Gbps). Finally, cell-switching can provide a broadcasting capability whereas circuit-switching can not. The benefits of using ATM are summarized below [1]:

- ATM technology is scaleable.

  An ATM cell can be transported over fiber or copper with a choice of line rates and framing protocols. The ATM standards simply specify the cell size, but do not mandate a line rate or a framing protocol. As a result, ATM cells can propagate over an Ethernet Local Area Network (LAN), then transit through gigabit ATM switches, and then get transmitted over DS3 lines. Thus ATM networks can serve the needs of users with a variety of equipment and a variety of bandwidth requirements.

•ATM technology is application transparent.

ATM is suitable equally for different applications such as voice, video, and data. All three kinds of traffic can exist in the same network and work seamlessly. ATM handles both delay sensitive traffic and loss sensitive traffic equally well without performance problems.

•ATM provides connection flexibility.

ATM nodes can be networked together in a variety of ways. One option may be to subscribe to a provider that sets up PVCs among the nodes. Another option may be to subscribe to SVC service that carries traffic from other subscribers. Pricing structures may be negotiated with the providers for use of bandwidth on a best-effort basis or on service guarantees,

•ATM is based on ATM Forum specifications.

There is a growing realization among equipment manufacturers that to be successful in the enterprise environment, equipment must interoperate. Network administrators feel that their investments in equipment will not be obsolete because of proprietary solutions provided by one vendor. The ATM Forum strives to promote interoperability of ATM equipment by developing specifications to promote interoperability.

2.1.3 ATM Reference Model

The ATM is based on the Broadband Integrated Services Digital Network (B-ISDN) service model. B-ISDN, in turn, relies on ISDN. The idea behind conventional (i.e. narrowband) ISDN is that a digital bit pipe exists between a customer and a carrier [2]. There are two types of digital pipes- the basic rate (BR) digital pipe and the primary rate (PR) digital pipe. Each of these pipes supports multiple channels that are interleaved by TDM. In the BR case, there are two 64 Kilobits per second (Kbps) digital pulse-code modulated (PCM) channels for voice or data (called B1 and B2 channels) and a 16 Kbps signaling channel (called the D channel) for out-of-band signaling. In the PR case, there are twenty-three B channels (each being a 64 Kbps channel) and one D channel also at 64 Kbps capacity. Since ISDN deals with 64 Kbps channels, it is called narrowband ISDN service. In contrast B-ISDN uses channel capacities much higher than 64 Kbps, namely, above 1.54 Mbps. Another important difference between ISDN and B-ISDN is that ISDN is a circuit-switched service (like a phone line), while B-ISDN is not. In other words, ISDN switches can not be used for B-ISDN switching.

The B-ISDN-based ATM reference model is shown in Figure 1. This model consists of three layers [2]: the physical layer, the ATM layer, and the ATM Adaptation Layer (AAL). The physical layer deals with electrical and optical parameters and bit timings in the physical

medium that transports the electrical signals. The physical layer consists of two sub-layers: the transmission convergence (TC) sublayer and the physical medium dependent (PMD) sublayer. The PMD sublayer provides physical interface to the cables and handles bit timings. The TC sublayer converts an incoming cell stream into bits at the ingress port and converts an incoming bit stream into a cell stream at the egress port. Thus the TC sublayer delineates cell boundaries and generates header check sums and verifies them. The next layer is the ATM layer, which provides some of the key functions of ATM [3]. The ATM layer generates and extracts ATM cell headers, provides VPI/VCI translation, and does cell multiplexing and demultiplexing. Finally, the AAL layer adapts data from higher layers into formats that conform to the ATM layer. Several different AAL data types have been defined by the ITU (e.g. AAL 1, AAL 3/4, and AAL 5). These are discussed in the following section. The AAL functions are end-to-end. The AAL layer is divided into two sublayers (Figure 2), the convergence sublayer (CS) and the segmentation and reassembly (SAR) sublayer. The SAR sublayer chops packets into cells (segmentation) at the source and puts them back into packets (reassembly) at the destination. The CS sublayer divides user data into manageable fixed-length packets called Protocol Data Units (PDUs).

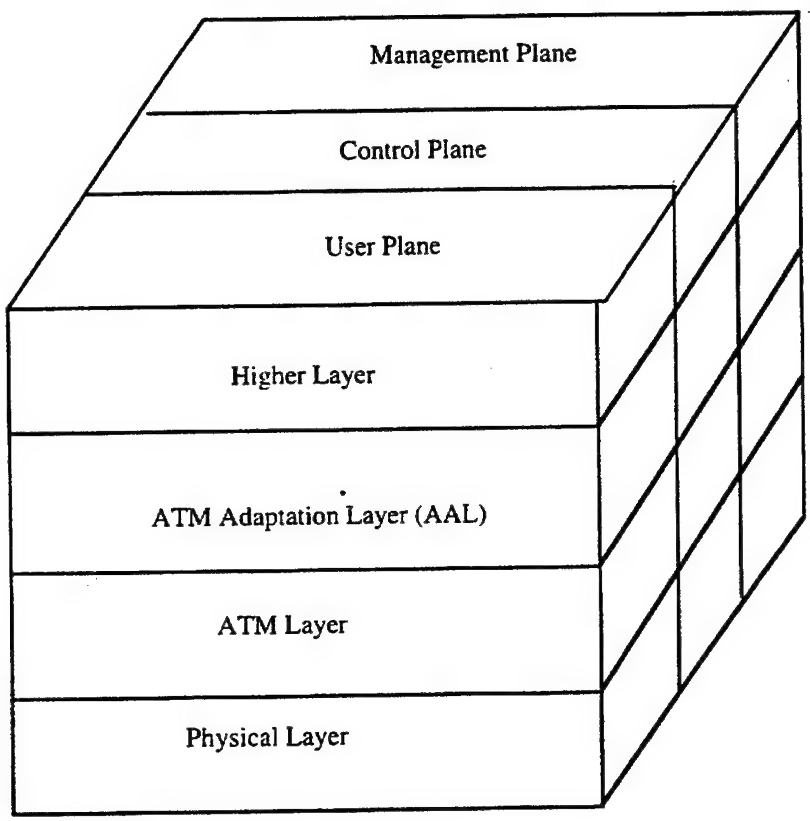
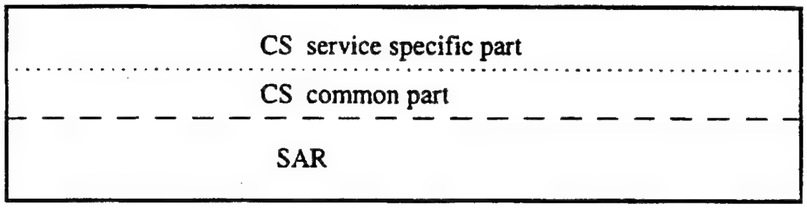


Figure 1. The B-ISDN ATM Reference Model



CS = Convergence Sublayer

SAR = Segmentation and Reassembly

Figure 2. The AAL Sublayers

In addition to the layers, the reference cube consist of three planes: the user plane, the control plane, and the management plane. The user plane spans the Physical Layer, ATM Layer, AAL Layer, and higher layers [3]. The higher layers run applications which interface with the AAL Layer via application programming interfaces (APIs). The control and management planes support the services provided by the user plane. The control plane supports control functions such as signaling and connection establishment. The management plane supports layer management and plane management. Layer management monitors user and control plane for faults, generates alarms, and initiates corrective action. Plane management performs coordination across all layers and planes.

2.1.4 ATM Traffic Classes

The ATM layer is insulated from the needs of user applications. Thus there is a gap between the user needs and the services provided by the ATM layer. The AAL layer bridges this gap. As its name implies, the AAL layer performs the functions needed to adapt the services provided by the ATM layer to the services required by applications. In an ATM network there are different AAL types, which support different traffic classes. ATM traffic classes, AAL types, and ATM QoS parameters are discussed.

There are five ATM traffic classes currently defined: Constant Bit Rate (CBR), Real Time Variable Bit Rate (RT-VBR), Non-real Time VBR (NRT-VBR), Available Bit Rate (ABR), and Unspecified Bit Rate (UBR). Each is discussed further below.

The CBR traffic class transmits bits at a constant rate. A Timing relationship between the source and destination is required. This traffic class covers important applications such as real-time uncompressed audio and video.

The RT-VBR traffic class supports time-sensitive services that transmit bits at a variable bit rate (VBR). An example of this traffic class is videoconferencing in which live video frames are compressed and transmitted. For this class of traffic, the ATM network must not introduce significant timing delays since this would distort the live pictures. Thus the delays in cell arrivals and their variances (called jitter) have tight bounds. This class of service is not loss-sensitive, implying that an occasional lost cell does not affect the quality of the picture.

The NRT-VBR traffic class transmits bits at a variable rate but without firm delay bounds. An application suited for NRT-VBR traffic class is multimedia-email. Another application is stored video.

The ABR traffic class is applicable to bit transmission that is bursty. Here, the network services are provided on a best-effort basis. The network provides maximum available throughput with minimum loss. In this service class a feed-back mechanism is in place to control the source behavior. An application suited for ABR traffic class is web-browsing.

In the UBR traffic class, the user sends traffic whenever it wants. An application suited for UBR traffic class is background file transfer. No guarantees or no feedback mechanism is in place. If there is congestion in the network, cells may be dropped. The sources do not reduce traffic during congestion.

2.1.5 AAL Types and QoS

Next we discuss the AAL layers that are in existence today. Currently there are four AALs defined.

- AAL 1: This layer is used for CBR traffic. The Common Part of the Convergence Sublayer (CPCS, Figure 2) performs the following functions: (1) It assembles and dis-assembles cells, (2) it compensates for delay variation of cells, and (3) it handles lost cells and provides for clock recovery. AAL 1 provides end-to-end timing in the network. It also aligns the application clock to the clock provided by the network.
- AAL 2: This layer is intended for ATM transport of compressed RT-VBR and NRT-VBR audio and video for connection-oriented traffic. A timing relationship between the sender and the receiver is needed. The Motion Picture Experts Group 2 (MPEG-

2) video encoding standard can be used for compression. Furthermore, AAL 2 can be used for bandwidth efficient transport of voice trunking.

- AAL 3/4: This is useful for traffic that is sensitive to loss but not to delay. AAL 3 /4 supports both connection-oriented and connectionless VBR traffic. Support for connectionless service is provided at the Service Specific Convergence Sublayer (SSCS) level. AAL 3/4 allows for multiplexing. Multiple sessions from a host can be multiplexed into a single virtual circuit and be transported over AAL 3/4. This layer can operate in message mode or streaming mode. In message mode, the boundaries of messages are preserved. However, in streaming mode, boundaries are not preserved. AAL 3/4 has two kinds of protocol overheads. A message gets a 4 octet overhead, whereas every cell gets an 8 octet overhead. Thus AAL 3/4 is not suitable for short messages.

- AAL 5: Just like AAL 3/4, AAL 5 supports both connection-oriented and connectionless VBR traffic. It also supports both message mode and streaming mode. However, AAL 5 is more efficient than AAL 3/4, since it has no cell overhead. AAL 5 can provide guaranteed delivery with flow control. It can also provide service with no guarantees. Thus AAL 5 is suitable for transport of IP packets.

The ATM traffic classes and the AAL types are closely related to another concept: QoS. It refers to a set of parameters that have been agreed upon between a user and a network to be guaranteed upon connection establishment. These parameters define the quality of service that the network will provide to the user. The agreement is called a traffic contract. As long as the traffic conforms to the agreed upon parameter set, QoS is guaranteed. Some of the important QoS parameters are listed below.

- Peak Cell Rate (PCR): This is the maximum number of cells per second that the user can send. The actual cell rate at any time may be less than the PCR. However under no circumstances may the instantaneous cell rate be greater than the PCR.

- Sustained Cell Rate (SCR): This is the time averaged cell rate the user is generating. For CBR traffic PCR and SCR are exactly equal. For bursty traffic, PCR will generally be much larger than SCR, i.e. PCR/SCR >> 1.

- Minimum Cell Rate (MCR): This is the minimum number of cell per second that the user is generating. If the cell rate in the network is less than the MCR, then the connection is unacceptable. For CBR traffic, MCR is again equal to the PCR. For ABR service, the bandwidth in any instant of time must be bounded by PCR and MCR. For UBR service MCR is set equal to zero.

- Cell Delay Variation Tolerance (CDVT): It represents the variation in cell transmission times. If CDVT = 0, then a network operating at PCR would deliver 1 cell every 1/PCR seconds. This means that the time between the first bit of a cell and the first bit of the next cell is exactly 1/PCR. For actual sources, this timing is not sustainable. As a result, there is the need for a parameter that takes into account variations in transmission time delays.

Additional QoS parameters that the network provides are given below.

- Cell Loss Ratio (CLR): This is the ratio of cells that are lost to the total number of cells that are transmitted.
- Cell Transfer Delay (CTD): This is the average time taken between the generation of the first bit of a cell at the source and the receipt of the last bit of a cell at the destination. This delay includes factors such as: coding delay, packetization delay, propagation delay, transmission delay, switching delay, queuing delay, and reassembly delay.
- Cell Delay Variation (CDV): This is a measure of how uniformly cells are delivered.
- Cell Error Ratio (CER): It is the fraction of cells that are delivered with one or more bits in error. A related quantity is the bit error ratio (BER). It is the ratio of number of bits in error to the total number of bits transmitted. Since fiber technology in ATM networks has made the networks very reliable, BER is an extremely small number.
- Severely-Errored Cell Block Ratio (SECBR): This is the fraction of a block of cells that contain an integer number M or more bits in error.
- Cell Misinsertation Rate (CMR): It is the number of cells per second that are delivered to a wrong address because of error in destination field of the cell header.

A traffic contract is introduced in the network by specifying some of the parameters mentioned above. The network uses two techniques to adhere to the traffic contract: *traffic shaping* and *traffic policing*. Traffic shaping refers to the process by which the network looks at the source behavior (such as PCR, SCR, and MCR) and buffers the traffic to reduce the PCR. Traffic policing (also called Usage Parameter Control (UPC)) refers to ensuring that sources stay within their negotiated connection setup parameters. The network can take corrective action to punish the violators. Some of these corrective actions include: marking the cells, dropping the cells, delaying the violating cells, and asking a source to correct the violation.

2.1.6 ATM Signaling and Addressing

ATM is a connection-oriented technology. A source that wishes to talk to a destination must establish a connection before data is transmitted. The types of service (e.g., ABR, CBR,

etc.) were discussed in the previous subsection. In this subsection we discuss signaling that is necessary to establish a connection. Signaling refers to a set of procedures and messages used for establishing an end-to-end connection between source and destination stations prior to information transfer. The types of signaling used in ATM networks are discussed below (see Figure 3).

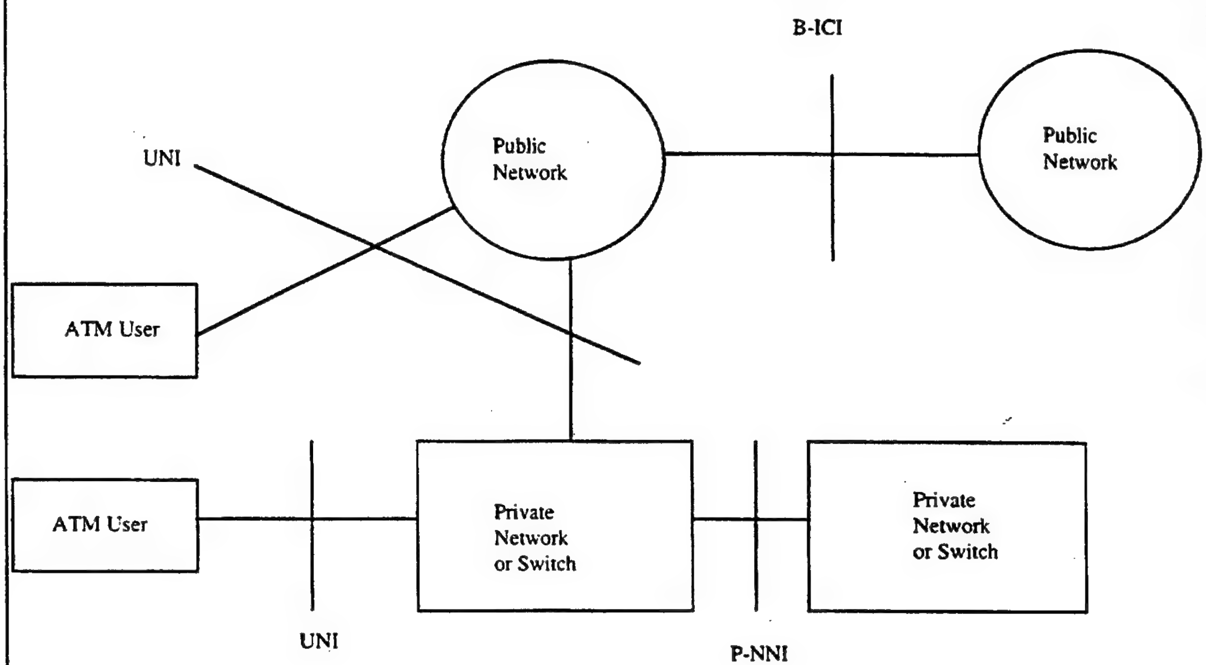


Figure 3. ATM Signaling Protocols

- User-to-Network Interface (UNI) Signaling:

  This signaling is used between an ATM end system (ES) and an ATM switch of an ATM network. The current specifications in ATM Forum's UNI signaling is UNI 4.0 specification. The earlier specifications in UNI signaling were UNI 3.0 and UNI 3.1. Most of the available UNI implementations are based on UNI 3.1 and vendors are migrating towards UNI 4.0. To initiate a call, a source ES sends a call Setup message with parameters such as destination address, QoS parameters, and traffic parameters to the ingress ATM switch. This switch invokes a Call Proceeding primitive. The switch invokes a routing protocol to propagate the request across the network to the egress switch. The egress switch then propagates the request to the destination ES. This ES then responds with a Connect message which propagates to the source ES

along the original path. The source ES receives and acknowledges the Connect message and data transfer takes place.

Some of the features of UNI 3.1 and UNI4.0 signaling are highlighted here. In UNI 3.1 signaling, the root ES can initiate point-to-point and point-to multipoint connections. The signaling channel is separate from the data transfer channel (in-band signaling). In UNI 3.1 signaling, the network can assign channels for data transfer. UNI 3.1 allows for error recovery and specifies UNI addressing formats.

UNI 4.0 signaling includes several new features to UNI 3.1 signaling. In UNI 4.0, a destination ES can request and join a point-to-multipoint call (leaf-initiated joins). It also supports the capability to negotiate channel numbers for data transfer. It supports QoS classes and also individual parameters for QoS classes. UNI 4.0 also supports anycast signaling (from a source ES to a leader of a group of ESs) and ABR traffic parameters.

- Network-to-Node Interface (NNI) Signaling: This signaling is used between switches or between networks. The signaling between two private switches is called Private NNI (P-NNI), whereas the signaling between two public switches is called Public NNI
- Broadband InterCarrier Interface (B-ICI)Signaling: This signaling is used between two public networks. For example, the signaling between a public switch of a regional carrier and a public switch of a long distance carrier is done using B-ICI.

Along with signaling protocols, the ATM Forum has specified formats of ATM ES addresses. For use within private ATM networks, the Forum has recommended the 20 octet ATM Network Service Access Point (NSAP) address format. For public networks, use of E.164 addresses is recommended. The Forum has also specified the NSAP encoding of E.164 addresses. In the United States, the local authority to assign NSAP addresses is the American National Standards Institute (ANSI) [4]. Within the DoD community, Defense Information Systems Agency (DISA) obtains the NSAP addresses from ANSI and assigns them to users. The NSAP addresses and E.164 addresses contain 6-octet end system identifier addresses which are typically the Ethernet addresses of the network interface cards. An ATM end system registers its NSAP address with a network switch using the Interim Local Management Interface (ILMI). This address registration process then greatly simplifies the establishment of a signaling connection across a UNI.

Up to this points we have discussed the basics of ATM. These basics included key concepts such as ATM traffic classes, AAL types, QoS, signaling and addressing. We next want to ask the ask the question of how to run applications in an ATM network? Since IP-based applications are the ones that are most commonly used, we discuss how IP is run over ATM in the next section.

2.2 IP and ATM

As discussed in the previous section, ATM provides signaling protocols to establish an end-to-end connection. ATM also provides QoS parameters for traffic management purposes. The AAL layers provide varying functionalities to adapt applications to the ATM network. However, to thrive in the market place, ATM must also enable commonly used IP applications to run transparently over ATM. The ATM Forum has actively pursued this area of work to integrate IP traffic into ATM networks. Two of the common methods of running IP in an ATM network are: Classical IP over ATM (put forth by the Internet Engineering Task Force (IETF)) and LAN Emulation (LANE). These are discussed in the following. This is followed by a discussion of MultiProtocol Over ATM (MPOA) which seeks to extend LANE.

2.2.1 Classical IP over ATM

To run connectionless IP datagram protocols over the connection-based ATM network, a scheme for encapsulating IP packets and for mapping IP addresses into ATM addresses is needed. Classical IP running over ATM achieves this in two main steps: packet encapsulation and address resolution. The most common method of packet encapsulation used is Logical Link Control / SubNetwork Access Point (LLC/SNAP) encapsulation [5] across an ATM AAL 5 connection. The resolution of IP addresses into ATM addresses is done using the method prescribed in Request For Comment (RFC) 1577 [6]. An address resolution protocol (ARP) is used to map the IP address either into an NSAP address or an E.164 address. RFC 1577 introduces the notion of a logical IP subnet (LIS) which is a set of IP hosts and routers that connect to a single ATM network and belong to the same IP subnet. Each LIS contains a single ATM ARP server. When a workstation starts up, it is connected to the ATM ARP server which registers its ATM address. If a host does not know the NSAP address of a IP destination, the ATM ARP server resolves that address. Upon receiving the NSAP destination address, the LIS client sets up a connection to that address. After a connection is successfully established to a destination, data is transferred across that connection.

Multicasting is supported according to the prescription given in RFC 2022 [7], which introduces the notion of a multicast address resolution server (MARS). Basically, a set of end points choose to use the MARS to register their membership. A sender has two options for sending multicast data to its members. The first option is to set up a point-to-multipoint VC with the group members as "leaves" and then send data from the sender as the "root". The second option for the source is to send data to a proxy multicast server which then sets up point-to-multipoint connections for transfer of data. FORE system's implementation of classical IP does not support multicasting at the present time. However, multicasting/broadcasting can be done via LANE which we discuss next.

2.2.2 LAN Emulation (LANE)

The second method of running IP applications over ATM is called LANE. It uses ATM as a backbone to interconnect existing LANs. In the LANE specification, there can be multiple logically separate LANs that work transparently as a single LAN over the same ATM network. A single emulated LAN (ELAN) emulates either an Ethernet or a Token Ring. It does not emulate a mixed Ethernet and Token Ring environment. Multiple ELANs may exist on a single ATM network because LANE does not emulate the collision detection algorithm of a legacy LAN.

Integration of LAN technology into ATM presents a challenge because LAN is a connectionless broadcast technology, whereas ATM is a connection-oriented non-broadcast technology. The ATM Forum's response to the challenge was to let every host establish ATM virtual circuits to every other host. This has the potential to proliferate the number of switched virtual circuits to unreasonable numbers.

The LANE v1.0 specification introduces three servers: LAN Emulation Server (LES), Broadcast and Unknown Server (BUS), and the LAN Emulation Configuration Server (LECS). These servers operate as follows:

- LES: The main function of the LES is address look-up. A host sends an Address Resolution Protocol (ARP) request to the LES asking for the IP address that is associated with an ATM address. The LES finds the IP address and sends it to the requesting host. This address is then used to send encapsulated packets to the destination.
- BUS: In a LAN, some applications use broadcasting to find unknown destination addresses. The BUS has virtual connections to all hosts in the emulated LAN. The BUS performs all broadcasting and multicasting and forwards unknown unicast addresses to a default gateway.
- LECS: The LECS entity assigns LANE clients to a particular emulated LAN. LECS provides configuration information and address of the LES.

If there are more than one ELAN, each of these ELANs must have its own LES/BUS entity pair. However, there can be only one LECS for the entire ATM network. Thus the LECS entity can be a single point of failure in the network. The issue of redundant LECSs is addressed in a new version, called LANE v2.0. This enhanced specification provides LANE capabilities such as logical link multiplexing, support for ABR QoS, enhanced multicast support, and support for MPOA.

2.2.3 MPOA

MPOA provides the connectivity of a fully routed environment taking as much advantage of ATM as possible. MPOA specification is a joint effort of the ATM Forum and the IETF. It

provides end-to-end connectivity across an ATM network, for hosts attached directly to the ATM network or indirectly through routers on IP subnetworks.

MPOA is an evolution of LANE. MPOA operates at both Layer 2 (just like a bridge) and at Layer 3 (just like a router). MPOA uses LANE for its Layer 2 forwarding. The key building blocks of MPOA are:

- LANE v2: This protocol is necessary to achieve Layer 2 forwarding.
- Next-Hop Resolution Protocol (NHRP): This is a protocol developed by the IETF and is used to achieve cut-through connection. Two neighboring hosts connected to a large ATM cloud may not realize that they are neighbors because of the way packets are routed. NHRP solves this problem by sending MPOA requests along the routed path to obtain ATM address information which then allows direct ATM virtual connections between MPOA devices.
- MARS: As already mentioned, MARS support the multicast and broadcast needs of Layer 3 protocols. MARS associates Layer 3 multicast group addresses with the ATM interfaces that are group members.

MPOA provides several benefits. It leverages existing infrastructure and allows for flexible changes in the network. Because of MPOA, there is no single point of failure in a wide area network. MPOA compliant products are available now.

2.3 Native ATM Services

As mentioned above, two of the methods of running IP-based applications over ATM are: classical IP over ATM and running IP with the use of LANE. None of the methods (including MPOA) take advantage of the unique benefits of ATM. Either an IP packet or an Ethernet frame has to be created and then overlaid on top of ATM.

Another possible mode of running applications over ATM is the native mode. This refers to an application interfacing with ATM protocols via ATM API syntax defined by the ATM Forum. Running an application in the native mode exploits all the unique features of ATM mentioned earlier.

Currently two ATM APIs have been specified. The Winsock Forum has developed Winsock 2 APIs for Microsoft NT operating system. The Open group has developed the XTI interface for Unix operating systems such as Solaris (Sun Microsystems) and Irix (Silicon Graphics). Both these APIs have been recognized by the ATM Forum as valid mappings of Native ATM Service Access Point (SAP) semantics. FORE systems provides the drivers for both Winsock2 and XTI APIs in their FOREThought (release 5.0 or higher) software for ATM switches.

Several products have been developed that use native ATM. A brief description of two such products are listed below. Both these products are multimedia applications.

- EMMI is a full-duplex Optical Carrier 3, concatenated (OC-3c) multimedia interface product of Lucent Technologies which uses ATM technology to simultaneously transfer audio and video over a LAN or a WAN. EMMI's audio sources consists of two independent stereo channels sampled at 44.1 Kilo Hertz (KHz) by analog-to-digital converter. The sampled information is buffered and processed according to AAL 1 and converted into a bit stream for transmission over the ATM network. The maximum audio bandwidth is 1.85 Mbps. EMMI's video source is a camera or video cassette recorder. The video source is sampled by the video analog-to-digital converter and buffered and encoded using the Joint Photographic Expert Group (JPEG) algorithm. The video information is then processed according to AAL 5 protocol and converted into bit stream for transmission over the ATM network. The video bandwidth has a range from 8 Mbps to 80 Mbps. The EMMI hardware can interface to a host such as a PC, a Macintosh machine or a Sun workstation for generation of data traffic which runs over a TCP/IP stack. The data is converted into the ATM cells using the AAL 5 protocol. The bandwidth usage depends upon the host system configuration. The EMMI interface is intended for applications such as real-time distance learning and tele-medicine.
- CellStack Video and Multi-point Control Unit (MCU) by K-NET Inc. (Plano, Texas), allows several sites across an ATM network to participate in an audio and video session. CellStack supports AAL 5 encapsulation for audio and video streams, and both PVC and SVC signaling. CellStack provides an OC-3c data path for transmitted and received ATM cells. For audio, the maximum bandwidth is 20 Kbps. For video, JPEG compression is used. The CellStack automatically registers the end-system address and generates the 20 octet NSAP address.

LiveLAN 3.1 by PictureTel Corporation is a H.323-based TCP/IP-based video-conferencing application for Personal Computers running Windows 95. PictureTel and FORE Systems are working together to develop and market a LiveLAN product that runs natively over ATM. This product is planned to be released in the first half of 1998.

In summary, we have presented an overview of ATM. We have reviewed ATM traffic classes, the types of ATM adaptation layers, and QoS parameters that the network will provide to the user. ATM signaling interfaces and addressing schemes are discussed. Two methods of running IP applications over ATM are discussed. In classical IP over ATM method specified by the IETF, a mapping of IP addresses into ATM addresses is done. In the LANE method specified by the ATM Forum, every host establishes ATM virtual circuits to every other host. The evolution of LANE into MPOA is also discussed. Finally, native ATM applications are discussed.

Section 3

3. Using ATM to Support ADS for T&E

In this section we present an example of how JADS might be able to utilize ATM. We also examine issues of concern to the JADS T&E community and provide approximate cost estimates.

The JADS ETE test consists of several phases of which phase two is examined in this paper. This phase tests the feasibility of ADS (which includes Distributed Interactive Simulation (DIS) protocol and the evolving Run Time Infrastructure (RTI) framework) to support Developmental T&E (DT&E) and Operational T&E (OT&E) [8]. This test scenario consists of five nodes (Figure 4). The Test, Control, and Analysis Center (TCAC) node is located at Albuquerque, New Mexico and is connected by dedicated T1 links to four other nodes. These nodes are: Fort Hood (III Corps), Texas; White Sands Missile Range (WSMR), White Sands, New Mexico; Grumman Aerospace Laboratory, Melbourne, Florida; and Fort Sill, Oklahoma. The ground station at Grumman is connected to the ground station at Fort Hood by a simulated Surveillance and Control Data Link (SCDL) at a T1 rate. Test control among participating sites is done via one voice channel on the T1 links.

1/1/1998

JADS End-to-End Test Phase 2 Topology

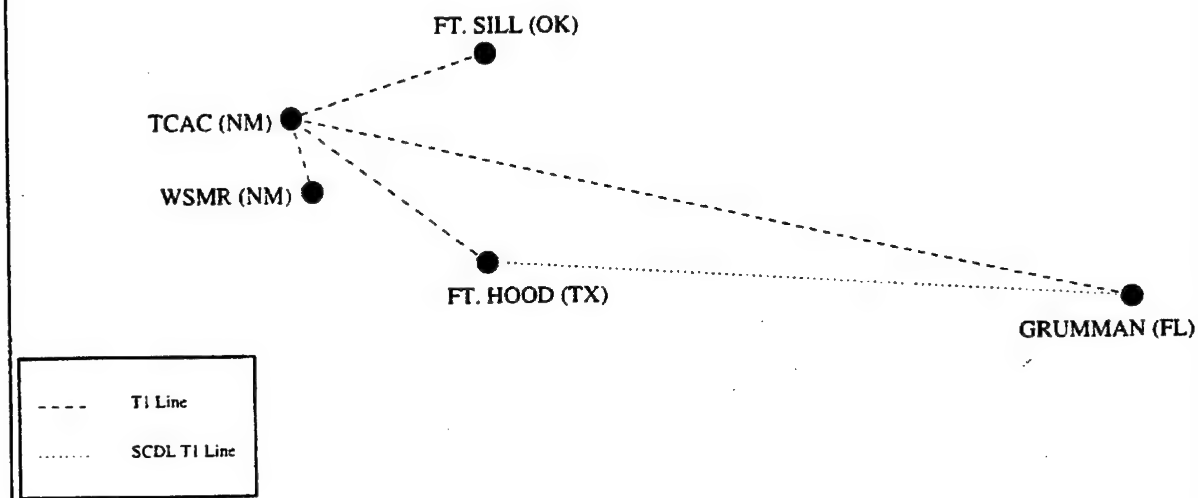


Figure 4. JADS Phase 2 ETE Test Topology

The network baseline requirements for running the JADS ETE phase two test are derived from engineering analysis of expected data traffic. These requirements are (based partly on correspondence with JADS ETE Test Team Lead Lt. Col. Mark McCall):

- The bandwidth (including voice) utilized in any given T1 link does not exceed 775 Kilobits per second (Kbps).
- The aggregate bandwidth exceeds 1.54 Megabits per second (Mbps) but does not exceed 3.08 Mbps.
- The upper limit of latency including allowable errors and radar timelines should be no longer than a second.
- The exercises are classified.

A potential configuration for running a phase 2 ETE test over an ATM network is shown in Figure 5 below.

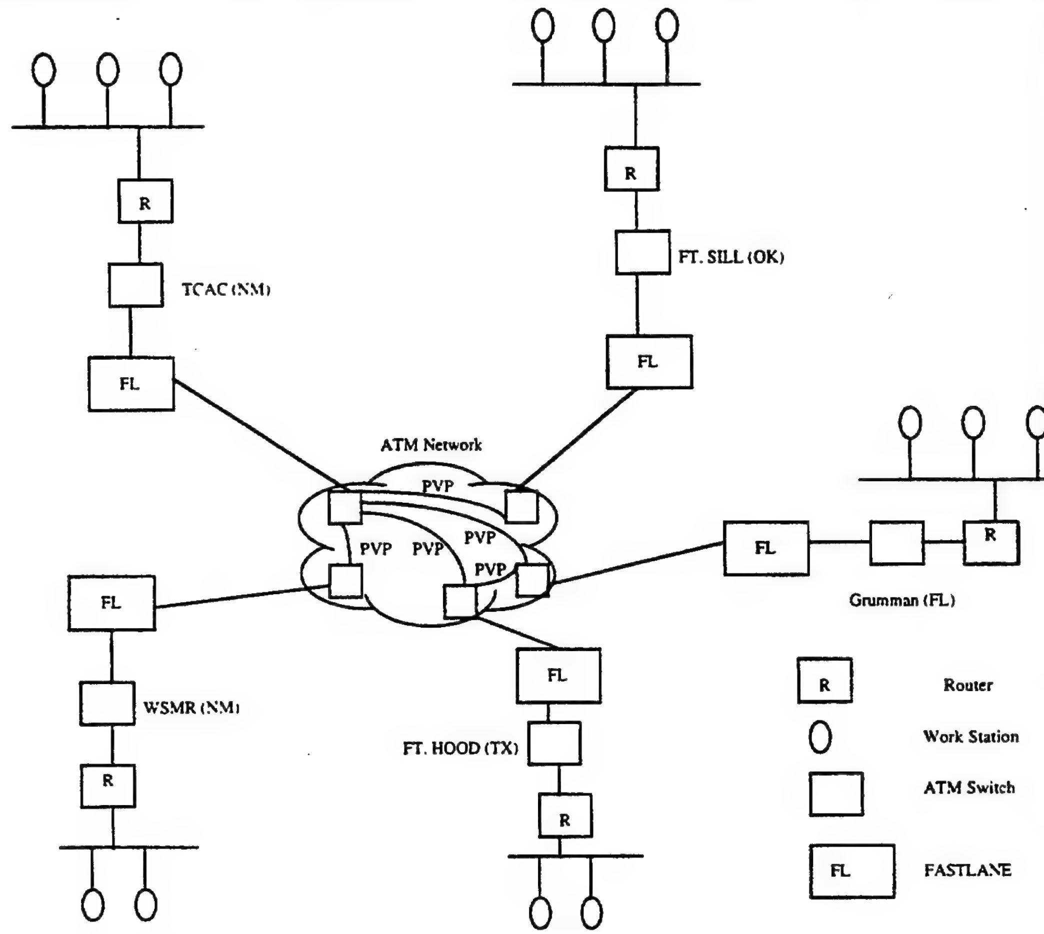


Figure 5. A Possible ATM Configuration for JADS ETE Phase 2 Test

We have made following assumptions in this configuration:

- Each LAN segment is connected to a router which is connected to an ATM switch (such as FORE ASX-200BX).
- Each ATM switch is connected to a FASTLANE built by GTE Corporation. The FASTLANE is approved by the National Security Agency (NSA) as a type 1 Key Generator-75 (KG-75) encryption device that can operate from Secret level to Top

Secret level. FASTLANE is the replacement for the low speed KIV-7HS bit encryptor that is currently used by JADS. FASTLANE understands ATM protocols and can support up to a total of 4096 cryptographically separated ATM connections. These connections can be combinations of PVCs and SVCs.

- The FASTLANEs are connected to service access points of a public ATM network.
- The five sites have 1.54 Mbps Permanent Virtual Path (PVP) connections as shown in Figure 5. A PVP is a collection of PVCs that can be setup among users.

3.1 JADS ETE Phase Two Test Over ATM

The JADS applications are launched in the workstations shown in Figure 5. The application generates simulation PDUs which are encapsulated in IP packets which communicate over the ATM network via LANE.

The following facts about this set up should be noted:

- Signaling: Connection is initiated between a switch and its user ES via UNI 3.1 signaling. A router and a switch initiate connection via the ILMI mechanism. Connection between a FASTLANE and its adjacent switches is initiated via UNI 3.1 signaling. At the present time FASTLANE doesn't support P-NNI signaling.
- Future FASTLANE release, due in March 1999, is expected to support P-NNI signaling.
- Addressing: As mentioned before, for the site switches, 20 octet NSAP addresses assigned by DISA may be used. The NSAP addresses will include the 6 octet globally unique Ethernet addresses. The emulated LAN interfaces (called asxn interfaces in FORE switches, n being an integer) can be assigned IP addresses as usual.
- LES/BUS and LECS: The LES/BUS and LECS functionality may be chosen to be configured in any site switch, say TCAC.

All the hosts are configured to belong to the same ELAN. After the initial connection set up, traffic flows as if the hosts are all on the same segment.

3.2 Issues and Solutions

ATM is an evolving technology, with specifications still in the process of refinement. It is natural to wonder if ATM network infrastructure is a good investment in terms of capital and technology. Some issues that JADS personnel have raised in this regard were listed earlier. They are again listed below followed by the answers.

- Would the ATM network be public or private? If public, what impact would other traffic have on latency of JADS data?

    The JADS community may choose a public ATM service provider to run their simulations. This choice does not impose any performance or security penalties. Data integrity and confidentiality is ensured through FASTLANE encryption devices and the use of PVP pipes.

    In the phase two ETE test scenario, latency is not an issue. The ATM network can guarantee much smaller latency over the wide area than the requirement of phase two ETE test. Typically, latencies in the network will be of the order of 100 msec or less. At the time of traffic contract negotiation between the user and the network, stringent delay bounds may be set up. The FASTLANE processes packets at nearly line speed and should not be a problem as far as latencies are concerned.

    The ATM network can be part of a DISA Federal network. Some of the other providers have Federal Networks for Government customers, to which JADS can subscribe. The cost estimates are provided in the next section.

- What are the encryption issues? How can encryption be accomplished between sites? Would we have to invest in NES rather than KIV-7?

    The low speed KIV-7HSs now used in JADS testing are bit encryptors working at the physical level. These boxes do not understand ATM. The KIV-7HSs should be replaced by FASTLANEs which understand ATM protocol including UNI signaling and transmit cells at speeds very close to the line rate. At the present time, Release 1 (R1) of a FASTLANE box with OC-3c interfaces, costs about $49 K. Release 3 (R3) of this box is scheduled for March 1999 and will cost $31 K. This will result in substantial cost reduction and will provide PNNI support. Another product in development by GTE is the TACLANE which encrypts either ATM cells or IP packets, but not both at the same time. TACLANE will provide throughputs of 4 Mbps for IP and about 45 Mbps for ATM. TACLANEs are scheduled to be available around December 1998. These units will cost about $9 K and will be easy to mount on racks.

- What are the bandwidth considerations?

    The switches and FASTLANEs have DS-3 ports and OC-3c ports. The bandwidth for DS-3 ports goes up to 45 Mbps and for the OC-3c ports goes up to 155 Mbps. As mentioned earlier, ATM is a scaleable technology. As the bandwidth needs increase, the network shall be able to handle these needs providing QoS guarantees. If the source traffic does not stay within the bounds specified in the traffic contract, cells may be dropped and data will be lost. If the users need more bandwidth, ATM rates become more economical.

- What are the latency considerations? Will latency be fixed or variable?

  The ATM network controls traffic through specification of QoS or UPC parameters. One of the UPC parameters is CDVT which is specified in units of microseconds. Thus the network provides for firm delay bounds. For CBR traffic, the latency will consist of fixed transmission delay and fixed propagation delay. For bursty VBR traffic, the aggregate delay will be variable. However, it can be guaranteed to have an upper bound.

- Will small packet size require more processing at simulation sites? Will this add variable latency equal to or greater than WAN savings?

  The ATM switches have a non-blocking switch fabric with speed of 2.5 Gbps. With these speeds the processing of cells is very fast. If Cisco routers with AIP cards are used, the fast packet switching option may be turned on. With traditional traffic loads (T1 or its multiples), and switch processing done in the hardware, the Central Processing Unit (CPU) utilization in switches and routers is rather small. The segmentation and reassembly done at the AAL layer will require more processing in the switches. However, with the backplane speeds mentioned above, additional latency is negligible. Even with encryption, the data throughput happens almost at the line rate.

- Will multicast be easier or harder with ATM?

  ATM protocols support multicasting. A root node in ATM can set up SVCs to all the leaf nodes of a multicast group. The membership of the group may be dynamic in the sense that the root node may add or drop leaf nodes. For IP-based traffic, the LANE protocol discussed earlier may be used to support multicasting. The establishment of an ELAN is quite straightforward. Initially, all members of the multicasting group need to set up connections to establish an ELAN. As long as the number of hosts in the group stays reasonable, LANE establishment is quite easy. LANE v1.0 does not support selective broadcast. This shortcoming has been removed in LANE v2.0.

- Will ATM be more or less reliable?

  In general, experience from Defense Simulation Internet (DSI) and DISA networks shows that ATM networks are pretty reliable. FORE's switch operating system, ForeThought 5.1 implements a distributed LANE environment which is claimed to minimize single point of failure. The network service providers have redundant switches which allow for reconfigurations in case of circuit failure.

- What are cost implications? Will T1 costs go up? Will new boxes be needed at simulation sites?

The recurring monthly charge for a T1 line is assumed to be in the range $1500 to $2500 depending on distance. The DISA service rate for ATM CBR traffic with a SCR of 1.5 Mbps is about $7 K per month. There is also a non-recurring charge of $1500 for initial site installation. Thus there will be cost increases by going through DISA service. ATM switches and FASTLANE encryption devices will be needed at the communication sites. The costs of these equipment are discussed in the next section.

- What are the cost implications for a private network? What would it take for us to build our own private ATM network (i.e. cost, equipment, training, etc.)?

  For T1 and dual T1 ATM pipes, the price difference between a public ATM network and a private ATM networks is expected to be marginal. For higher bandwidth pipes (such as DS3 pipes), and multiple users at a site, there will be substantial savings (up to 50%) in going via a public ATM network [9]. The cost of equipment is discussed in the next section. Because of resource constraints, investigation of training costs and detailed cost implications of private ATM networks could not be made.

In summary, ATM technology is quite capable of meeting the requirements of the JADS community. Since the cost of equipment and services is a major concern, we make a cost analysis in the next section to give a feel for the expenses involved.

3.3 Cost Analysis

In this cost analysis we have picked standard equipment used in modern networks and looked at their costs without attempting to make an exhaustive product comparison.

- The list prices for FORE ASX-200BX switch components are: chasis (switch fabric, 4 empty slots, redundant power supply, and 1 switch control processor) $16K; a DS-1 module with 4 ports $5 K; a DS-3 module with 4 ports $14 K. For Federal Government customers, FORE discounts list prices by 16%. Thus the discounted price for an ASX-200BX switch with a 4 port DS-1 module would cost about $18 K.
- An ASX-BX200 switch with a 4 port OC-3 module for multimode fiber would cost about $16.5 K (including discounts).
- Workstations that run the simulation applications may be connected to a router which in turn can be connected to a switch. Alternately, workstations may be equipped with ATM network interface cards (NIC). These cards are available for Peripheral Components Interconnect (PCI) bus or S-bus interfaces. Typically, an ATM NIC card costs less than $1 K (Efficient Networks is one vendor that manufactures NIC cards).

- For traffic encryption, FASTLANE boxes are used. A FASTLANE with DS-1 or DS-3 support costs about $47 K and includes the cost of upgrade to Release 3 due in March 1999. Thus the FASTLANEs are a big component of the cost structure. The Release 3 of the FASTLANEs will be cheaper, costing around $31 K as already mentioned.
- The unofficial DISA service rate for CBR traffic with a SCR of 1.5 Mbps is about $7 K per month ($6 K for 1 Mbps) for each pipe. There is also a non-recurring charge of $1500 for initial site installation. The advantage of ATM becomes transparent if higher bandwidths are needed. At this point the cost savings for the monthly access charges become substantial. For example, a traffic contract for a SCR of 5 Mbps CBR traffic costs only $8.5 K per month.

Section 4

4. CONCLUSIONS

In this paper we have reviewed some aspects of ATM technology that may be of interest to the JADS community. We have discussed the benefits of ATM internetworking. We have also presented key concepts such as ATM service classes, AAL types, and QoS. We have discussed ATM signaling protocols and the ATM addressing structure. The options for transporting IP traffic over an ATM network have been discussed. The availability of native ATM services for voice and video has also been discussed.

We have considered a particular JADS ETE test scenario and have examined its feasibility of being run over an ATM network. Questions of specific interest to the JADS community, such as latency, bandwidth, and multicasting have been addressed. Finally approximate cost estimates of components and service charges have been given.

From a financial point of view, it would seem that a public ATM network for JADS is not cost-effective as compared to dedicated T1 lines and KIV-7HS bit encryptors in existence now. One big item in the expense column is the high-speed FASTLANE encryptor which replaces KIV-7HS. Another big-ticket item is the ATM switch. As already mentioned, the cost of these boxes is expected to go down in future. Furthermore, alternate boxes may be available in future, which are substantially cheaper and do several levels of encryption. Leaving aside the cost factor, we recommend that ATM network be chosen to carry the JADS simulation data. Advantages of ATM such as QoS guarantees, scaleability, fast processing, fast propagation, and firm delay guarantees make ATM very attractive. Ongoing developments in voice and video will make this technology even more attractive in future.

Finally, we mention two areas of further investigation. One area of study is an investigation of running ADS applications directly over ATM. A practical example of how this can be achieved and the benefits that will result is an important area of research. The other area of study is the cost of setting up a private ATM network for JADS. Such a study should include the recurring line charges as a function of bandwidth and the cost of training. It is hoped that as ATM becomes more popular in the future, the capital outlays and service charges become more affordable.

List of References

1. Telco Systems, "Asynchronous Transfer Mode: Bandwidth for the Future", 1992.
2. Tannenbaum, Andrew S., "Computer Networks", Third Edition, Prentice Hall PTR, New Jersey, 1996.
3. McDysan, David E. and Spohn, Darren L., "ATM", McGraw Hill, New York, 1995.
4. Alles, Anthony, "ATM Internetworking", Cisco Systems, 1995.
5. Heinanen, Juha, "Multiprotocol Encapsulation over ATM Adaptation Layer 5", Request For Comment (RFC) 1483, 1993.
6. Laubach, M., "Classical IP and ARP Over ATM", Request For Comment (RFC) 1577, 1994.
7. Armitage, G., "Support for Multicast over UNI 3.0/3.1 based ATM Networks", Request For Comment (RFC) 2022, 1996.
8. Sahu, Devaraj, "A Study of the Defense Simulation Internet (DSI) for the Joint Advance Distributed Simulation (JADS) Project", MITRE Report, April 1998.
9. Yocum, Bernard, Houston Associates, Inc.{703-284-8724}, in telephone conversation, April 14, 1998.

Glossary

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ADS	Advanced Distributed Simulation
ANSI	American National Standards Institute
API	Application Programming Interface
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BER	Bit Error Ratio
B-ICI	Broadband InterCarrier Interface
B-ISDN	Broadband Integrated Services Digital Network
BR	Basic Rate (in ISDN)
BUS	Broadcast and Unknown Server
CBR	Constant Bit Rate
CDV	Cell Delay Variation
CDVT	Cell Delay Variation Tolerance
CER	Cell Error Ratio
CLR	Cell Loss Ratio
CMR	Cell Misinsertion Rate
CPCS	Common Part of Convergence Sublayer (an AAL sublayer)
CPU	Central Processing Unit
CS	Convergence Sublayer (an AAL sublayer)
CTD	Cell Transfer Delay
DIS	Distributed Interactive Simulation
DISA	Defense Information Systems Agency
DS1	Digital Signal Level 1 (1.54 Mbps)
DS3	Digital Signal Level 3 (44.74 Mbps)
DSI	Defense Simulation Internet
DT&E	Developmental Test and Evaluation
ELAN	Emulated LAN
ES	End System
ETE	End-to-end
EW	Electronic Warfare
FY98	Fiscal Year 1998

Gbps	Gigabits per second
HLA	High Level Architecture
IETF	Internet Engineering Task Force
ILMI	Interim Local Management Interface
IP	Internet Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
JADS	Joint Advanced Distributed Simulation
JPEG	Joint Photographic Expert Group
Kbps	Kilobits per second
KG-75	Key Generator 75
KHz	Kilo Hertz
LAN	Local Area Network
LANE	LAN Emulation
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LIS	Logical IP Subnet
LLC	Logical Link Control
MARS	Multicast Address Resolution Server
Mbps	Megabits per second
MCR	Minimum Cell Rate
MCU	Multipoint Control Unit
MPEG-2	Motion Picture Expert Group 2
MPOA	Multiprotocol Over ATM
NHRP	Next Hop Resolution Protocol
NNI	Network-to-node Interface
NRT-VBR	Non Real Time Variable Bit Rate
NSA	National Security Agency
NSAP	Network Service Access Point
OC-3c	Optical Carrier 3, concatenated
OSD	Office of the Secretary of Defense

OSPF	Open Shortest Path First
OT&E	Operational Test and Evaluation
PCI	Peripheral Components Interconnect
PCM	Pulse Code Modulation
PCR	Peak Cell Rate
PDU	Protocol Data Unit
PIM	Protocol Independent Multicasting
PMD	Physical Medium Dependent (a sublayer of ATM physical layer)
P-NNI	Private Network-to-node Interface
PR	Primary Rate (in ISDN)
PVC	Permanent Virtual Circuit
PVP	Permanent Virtual Path
QoS	Quality of Service
RFC	Request for Comment
RT-VBR	Real Time Variable Bit Rate
RTI	Run Time Infrastructure
SAP	Service Access Point
SAR	Segmentation and Reassembly (an AAL sublayer)
SCDL	Surveillance and Control Data Link
SCR	Sustained Cell Rate
SECBR	Severely-Errored Cell Block Ratio
SIT	Systems Integration Test
SNAP	Subnetwork Access Point
SSCS	Service Specific Convergence Sublayer (an AAL sublayer)
SVC	Switched Virtual Circuit
T1	System that transports Digital Signal Level 1 (1.544 Mbps)
TC	Transmission Convergence (a sublayer of ATM physical layer)
TCAC	Test, Control, and Analysis Center
TDM	Time Division Multiplexing
T&E	Test and Evaluation
UBR	Unspecified Bit Rate
UNI	User-to-network Interface
UPC	Usage Parameter Control
VBR	Variable Bit Rate

VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VPC	Virtual Path Connection
VPI	Virtual Path Identifier
WAN	Wide Area Network
WSMR	White Sands Missile Range

Distribution List

Internal

Internal

W010

J. S. Quilty

W110

J. C. Slaybaugh

W150

H. J. Carpenter
R. Eftekari

W15D

J. S. Dahmann

W15E

C. E. Walters (5)
E. R. Gonzalez (10)
G. A. Tsoucalas
F. R. Richards
M. Hammond
Files (2)

W15F

M. Adams
S. Chakravorty
D. Sahu (5)
N. Schult

W062

N. J. Slattery
S. Welman

Records Resources (3)

External

Office of the Under Secretary of Defense
(Acquisition)
Deputy Director, Test,, systems Engineering &
Evaluation/Systems Assessment
ATTN: Lt. Col. Steven Cameron
The Pentagon, Room 3D1080
Washington, DC 20301-3110 (5)

Colonel Mark Smith
JADS Joint Test Director
JADS JTF
11104 Menaul Blvd., NE
Albuquerque, NM 87112 (10)

Appendix E

SIPRNET Customer Connection Process

SIPRNET
CUSTOMER CONNECTION PROCESS

27 July 1999

DISN Network Services/D3124
11440 Isaac Newton Square
Reston, Virginia 20190-5006

There are three major efforts a customer must be concerned with to obtain direct SIPRNETconnectivity. These are identified within this document and are as follows:

Initial Modeling Request – Found on page 14
Request For Service (RFS)
Security Accreditation Documentation.

These items are explained more thoroughly further on within the instructions.

SIPRNET Points of Contact:

Program Manager:

Mrs. Cindy Moran- 703-735-8259 / D3124

Customer Service Manager:

Mr. Jim Nostrant - 703-735-3238 / D3124 - nostranj@ncr.disa.mil

Customer Service Representative for Army and Navy

Mr Johnnie (Jay) Johnson – 703-735-8130 / D3124 – johns10j@ncr.disa.mil

SIPRNET Security Manager:

Mr. John Staples - 703-735-3236 / D3124 – staplesj@ncr.disa.mil
(Security Accreditation Packages)

Waivers:

Ms Betty Lewis – 703-735-8168 - D3Waive@ncr.disa.mil

SIPRNET ACCESS CHECKLIST:

To ensure you are able to obtain connectivity to the SIPRNET please complete the following checklist as you go through the process.

Have you contacted the SIPRNET PROGRAM MGMT OFFICE? (In the event you received this checklist without the remainder of the SIPRNET CUSTOMER CONNECTION PROCESS)	Yes / No
CONTRACTORS ONLY – Has your Sponsor contacted Joint Staff regarding validation of your requirement To have connectivity to SIPRNET?	Yes / No
NON DOD ONLY – Have you contacted Joint Staff Regarding validation of your requirement to have Connectivity to SIPRNET?	Yes / No
CONTRACTOR ONLY – Have you been in contact with Defense Security Services (DSS) regarding Security Accreditation Package?	Yes / No
Have you submitted Initial Modeling Request (IMR) to SIPRNET to obtain "B" Side information for your connection?	Yes / No
Have you received "B" Side information back from SIPRNET office?	Yes / No
Have you, or your Sponsor in the case of Contractor Connections, submitted Request For Service (RFS) To your supporting Telecommunications Certification Office?	Yes / No
Have you, with the exception of contractor connections which go through DSS, submitted Security Accreditation Package to SIPRNET?	Yes / No
Has Telecommunications Service Request been Issued for you requirement?	Yes / No
Has Telecommunications Service Order (TSO) been Issued for your requirement?	Yes / No
Do you have customer premis equipment for connection to the SIPRNET?	Yes / No
Have you obtained backside IP Addresses from SIPRNET SUPPORT CENTER? (If Applicable)	Yes / No

SIPRNET CUSTOMER CONNECTION PROCESS

1. Initially the customer will contact Mr. Jim Nostrant , Mr Jay Johnson or Mrs. Cindy Moran to obtain information regarding the SIPRNET and procedures for connection to the Network.

2. As the primary customer contact for SIPRNET customers, Mr Jim Nostrant will be POC for SIPRNET connectivity.

3. During initial conversation with customer, arrangements should be made to provide the customer the current information package. At present it consists of the following.

A. Current billing rates for connectivity.
B. Information pertaining to the Security Accreditation Package which customer needs to complete and return. It should be noted that this is not a sample Security Package.
C. Initial Modeling Request form.

4. When speaking with the customer SIPRNET personnel must ensure customer understands specific items relating to connectivity to the SIPRNET. These must consist of, but are not limited to the following:

A. There is an approximate **120** day lead time from date **TSR** issued prior to connectivity to the network.

1. There are individuals within the organization who advocate approximately 30 days. This is a valid goal but at this juncture it is simply not possible on a regular basis.

2. Effective immediately connections WILL NOT be activated until such time as an IATC has been issued by D3124. Connection will be made as normal but will not be activated. In addition, customer may be billed for connectivity effective this date. Exceptions to this will be on a case by case basis through the J6.

a. Customer must allow a minimum of **60** days for evaluation of submitted security package prior to intended activation date.

B. Requirement for site survey, (normally done by contractor) of host location.

1. Customer location site survey is normally NOT done.

2. There are, in fact, some locations, although very few, which could possibly require a site survey.

3. Due to scheduling requirements those locations requiring a survey may have delay in implementation and incurred cost may be passed to the customer.

C. Requirement of customer to coordinate with their specific COMSEC Custodian for issuance and delivery of KIVs or KGs and keying material to host location.

1. This is to be completed so Crypto Equipment and keying material will be on site prior to FE visit for installation. DISA WILL PROVIDE the required KIVs or KGs and CSU/DSUs based on speed requirements.

a. 64KB or less the general rule of thumb will be KG-84 with CODEX CSU/DSU at user location.

b. 128kb or above would be KIV-7HS supported by Larscom CSU/DSUs

D. Requirement for customer to complete installation of their host equipments. DISA (Contractor Support) is only required to complete installation up too the Red side of KIV/KG. Cableing and connectivity from Red side KG to host equipment is the responsibility of the customer.

1. Host hardware and software is to be installed prior to visit by contractor to actually complete installation to the SIPRNET. At least to the extent that connection can be tested. In this fashion DISA will eliminate the frequency of multiple visit to same location at various stages of the activation. Customers must also understand that DISA does not provide customer Premise routers. Majority of existing customers have connected some type of router to the SIPRNET. Those that elect to connect other equipments such as workstations etc must realize that whatever equipments they elect to connect must support TCP/IP.

E. For Ethernet type connections it is the responsibility of the customer to provide and install cabling up to the SIPRNET Hub router. FE will normally not be sent on these installation/activations. Customer must remember that this Ethernet path is Red and must be protected as such.

F. Network Delay - There is a 300 millisecond delay one way within theatre incurred on the SIPRNET or 600 millisecond round trip. When going between theatres such as a connection from Europe to CONUS this number would be 600 milliseconds one way (1200 roundtrip). This is a worst case scenario.

G. All customers must be DOD Government Service or Agency. Any private contractor connections must be sponsored by a DOD government service or agency. (See Item 11)

1. Network connections of Non DOD Government Agency or contractor sites must be validated through J6. For contractor requirements the sponsoring Service or Agency has the responsibility of contacting J6. The J6 point of contact is Major Gary Klabunde at (comm) 703-697-7091.

2. Contractor connections must also go through the Defense Security Service, DSS, for accreditation of their facilities. This is to include direct connections to the SIPRNET.

H. Depending upon the type of connection and the number of "backside hosts", the customer may or may not be required to obtain an Autonomous System Number (ASN). This can be determined by contacting the SIPRNET Support Center (SSC) 1-800-582-2567 / 1-703-821- 6260. If needed, the customer can obtain an ASN by going thru the SSC.

I. Requirement for customer to provide the "backside" IP address. We will provide the network address (e.g., 140.049.XXX.XXX) for the actual connection to the network. It is the customers responsibility to obtain/provide the addressing to the backside of their premise equipments. This is required prior to being able to activate the connection. If customer does not already have these addresses they may be obtained from the SIPRNET Support Center.

NOTE ALL BACKSIDE IP ADDRESSES UTILIZED ON THE SIPRNET MUST BE REGISTERED WITH THE SIPRNET SUPPORT CENTER. NIPRNET IP ADDRESS ARE NOT AUTHORIZED FOR USE ON THE SIPRNET.

a. The exception to this rule are those connections to a contractor facility. To obtain their backside IP Addresses contractor sites must contact Mr Bill Ishmael or Mr Larry Moore at disn@mail.dss.mil

J. Specific items related to obtaining circuit path to customer locations. On numerous installations it has been found that the most difficult portion of the connection becomes the last 50 feet. This is normally from the commercial demarcation point to the host. Ie: the local GFE path. In some instances this is a contractor

supported/maintained path with site specific methods for completion. We need to know of potential problems associated with the completion of this portion of the connection. This would include a local POC at the base/camp or station who should be coordinated with in the TSR/TSO process. This information could very well be the difference between a successful completion and an extended delay.

5. When the customer returns the completed Initial Modeling form to D3113 the following actions will occur.

A. SIPRNET personnel sends E-Mail request to modeling function to determine the following.

1. SIPRNET Hub to which customer connection will be made.
2. IP Address assigned to customer. ie: 140.049.XXX.XXX

6. Once modeling provides items 1 and 2 back this information is passed to the customer. This should normally be within 48 hours of receipt of Initial Modeling Effort form from customer.

7. Customer submits Request For Service (RFS) to their respective supporting Telecommunications Certification Office (TCO) for the issuance of the Telecommunications Service Request (TSR).

Please ensure the following PLA address is included when sending RFS.
(DISN SPT CONTRACTOR WASHINGTON DC//T1/T2/ITA//)

IMPORTANT

TO ENSURE REQUIREMENT IS PROCESSED PROMPTLY PLEASE CONTACT JIM NOSTRANT AS SOON AS RFS IS RELEASED. IN ADDITION, PLEASE FAX COPY OF RFS TO JIM AT (comm) 703-735-8343/8482 (dsn) 653-8343/8482.

A. As this is an encrypted Network when submitting RFS customer MUST remember to include COMSEC information.

1. COMSEC Account Number
2. COMSEC Custodian=s Name
3. COMSEC Custodian=s Phone Number
4. PLA for Comsec Custodian
5. Mailing Address for COMSEC Custodian

B. There are some slight variations within this process determined by supporting TCO:

1. Army TCO wishes to have the customer contact them prior to the modeling process. Army TCO desires that they be the point at which the AB@ side information is requested. This is not to say that DISA cannot speak with the customer.

   a. B side information is that location where the customer connection actually connects directly to the SIPRNET. If a customer connects to the backside of an existing SIPRNET host they are considered a backside connection and not a true SIPRNET customer.

2. Air Force has requested that all of their requirements go through the Air Force Systems Networking Program Office. (AFSN) at Gunter AFB. DISA will continue to work with customers as previously explained but customer is to send their request for B side information through the AFNSC.

   a. POC is Mr. Walt Jones
   b. Phone © 334-416-6107 (d) 596-6107
   c. FAX is © 334-416-1040 (d) 596-1040
   d. E-Mail is wjones@ddn.af.mil

4. The following are willing to go with customer obtaining B side information from this office.

a. Navy/Marine
b. Other miscellaneous DOD organizations.

1. ie: NIMA, MSC, etc.

8. Upon receipt of Modeling information D3124 will notify customer of B side. This is the specifics as to which Hub and port assignments have been assigned against this connection requirement.

9. Upon receipt of TSR, D3124 knows funding has been applied to requirement. At this point it should be approximately 120 days for connectivity. Once TSO is received the requirement is actually placed on the Master Schedule for implementation/activation.

A. Regardless of ROD date identified, requirement will not be placed on Master Schedule any sooner than 8 weeks from date TSO received by support contractor. It takes up to 6 weeks to obtain keying material once TSO has been issued. If placed on Schedule for a date prior to arrival of key at customer location installation must be slipped thus disturbing the Master Schedule unnecessarily.

10. Once D3124 receives the customer's Security Accreditation documentation the following actions occur.

A. D3124 will review documentation for accuracy and completeness.

B. If all requirements are satisfied, the package will be sent to DISA/D251 for a certification determination. If package is complete D251 will recommend to D3113 that IATC be issued.

C. D3124 will issue IATC and allow the connection to be made.

D. D251 will complete on line compliance testing.

E. Upon successful completion of Compliance Testing D251 informs D3124 of results and D3124 issues the Final Approval to Connect (ATC).

11. FOREIGN NATIONAL CONNECTIVITY - (See Information Paper)

12. SIPRNET SUPPORT CENTER - 1-800-582-2567 / (703) 821-6260

13. SIPRNET RATES:

ALL THEATRES IP ROUTER SERVICE - MONTHLY RECURRING CHARGES / FY99

BANDWIDTH:	ETHERNET	9.6	19.2	*56/64	128	256	512	1024 - T1	E1
CONUS	7,748	1,033	1,033	1,033	1,808	3,099	5,165	6,198	n/a
EUROPE	10,304	1,288	1,288	1,288	2,254	3,864	6,440	7,728	8,372
PACIFIC (HA/AL)	7,748	1,033	1,033	1,033	1,808	3,099	5,165	6,198	n/a
PACIFIC RIM	10,800	1,350	1,350	1,350	2,363	4,050	6,750	8,100	n/a

*56KB AVAILABLE IN CONUS, 64KB FOR O'CONUS CONNECTIVITY.

**NON RECURRING CHARGES FOR INSTALLATIONS: $2,500 FOR < AND $5,000 FOR > OR = TO 512KBS.

*** DIAL-UP SERVICE = $50 INITIATION FEE PLUS $27 PER MONTH PER COMM SERVER ACCESS CARD.

**** DUAL HOMING - SECOND CONNECTION OF DUAL HOMED SYSTEM WILL BE CHARGED 50% OF THE MRC THAT THE SECOND CONNECTION LINE SPEED WOULD ORDINARILY PROMPT.

****THE MANAGEMENT OF CUSTOMER PREMISE ROUTERS (CISCO OR WELLFLEET ROUTERS) HAVE A FLAT FEE OF $50.00 PER MONTH FOR ALL NEW CUSTOMERS IN FY96 AND FOR ALL CURRENT CUSTOMERS IN FY97. ALL OTHER ROUTER MANAGEMENT (NOT CISCO OR WELLFLEET) WILL REQUIRE A SPECIFIC COST ESTIMATE TO DETERMINE A FEE.

14. SIPRNET RATES – MEET ME BILLING

IT SHOULD BE NOTED THAT THE FY98 AND FY99 RATES HAVE REMAINED THE SAME WITH ONE EXCEPTION. THEY HAVE BECOME FURTHER DEFINED AS TO WHAT LOCATIONS WITHIN THE EUROPEAN AND PACIFIC THEATRES, THE FLAT RATE CONNECTION CHARGES WILL BE APPLIED TO. FOR THOSE AREAS NOT IDENTIFIED BELOW, MEET ME BILLING WILL APPLY. MEET ME BILLING IS WHERE THE CUSTOMER IS RESPONSIBLE FOR THE COST OF ACCESS CIRCUIT TO THE DISN NODE PLUS THE RATE FOR THE ORDERED DISN SERVICE. (CONNECTION CHARGE) ADOPTING A "MEET ME BILLING" APPROACH IS A FUTURE STEP IN ADOPTION OF COMMERCIAL TYPE BILLING FOR THE DISN SERVICES AS MANDATED BY ASD(C3I) AND USD(C).

EUROPEAN RATES:

AZORES
BELGIUM
BOSNIA
GERMANY
ICELAND
ITALY
SPAIN
TURKEY
UNITED KINGDOM

PACIFIC RATES:

AUSTRALIA
GUAM
DIEGO GARCIA
JAPAN
OKINAWA
KOREA

MEET ME BILLING: IN FY 1999, MEET ME BILLING WILL APPLY TO OUR SERVICES ORDERED WHICH EXTEND TO COUNTRIES OUTSIDE OF THE THEATRES DEFINED ABOVE. IN FY 2000, MEET ME BILLING WILL APPLY TO ALL CONNECTIONS.

15. BACKSIDE CONNECTIVITY / LONG HAUL POLICY

The following message is referring to those local connections to the backside of a SIPRNET customer' host. For example, a host front end to a base Red LAN. Those on base connections would be acceptable but off base connectivity would not normally be allowed.

ROUTINE

R 121734Z AUG 97

FM DISA WASHINGTON DC//D3//

TO DISA WASHINGTON DC//D3//
HQ USAF WASHINGTON DC//SCM//
CMC WASHINGTON DC//C21/POC-30/C412//
HQDA WASHINGTON DC//SAIS-C4X//
CNO WASHINGTON DC//OP941/N61/N62//
NIMA HQ FAIRFAX VA//TSC//
HQ DNA WASHINGTON DC//NOCC//
DIA WASHINGTON DC//DS/CISA/SYS//
DLA FT BELVOIR VA//CAN//
DIRNSA FT GEORGE G MEADE MD//Q11/Q21/Y414/Y44/CIO//
NRO WASHINGTON DC//COM//
ONI WASHINGTON DC//O7//
DECA FT LEE VA//
SECDEF WASHINGTON DC//BMSO/USDP-DSAA/ASD-GC//
USCINCTRANS SCOTT AFB IL//TCJ6/USTC/J2-PY//
CINCUSACOM NORFOLK VA//J63/ACJ6//
USCINCEUR VAIHINGEN GE//ECJC//
USCINCSTRAT OFFUTT AFB NE//J6//
USCINCSO SCJ1 QUARRY HEIGHTS PM//
USCINCSPACE PETERSON AFB CO//J6//
USCINCCENT MACDILL AFB FL//J6//
USCINCSOC MACDILL AFB FL//J6//
USCINCPAC HONOLULU HI//J6//
JOINT STAFF WASHINGTON DC//J6T//
SECDEF WASHINGTON DC//C3I//
CDRUSAIC FT HUACHUCA AZ//STZS-IMI-T//
HQ AFCIC WASHINGTON DC//SYN//
AFPCA WASHINGTON DC//SMT//
PEOCMPANDUAV WASHINGTON DC//PEOCU-B22//
HQ SSG MAXWELL AFB GUNTER ANNEX AL//SIN/SCMGU//
NCTAMS LANT NORFOLK VA//N3/N33/N33D/N33N/12//
DRPC PAC PEARL HARBOR HI//PCR34//
NCTAMS EASTPAC HONOLULU HI//N34//
CDROPMAS-E DCS STA LANDSTUHL GE//ASQE-F-ITT-LDL//
CDR5THSIGCMD RFS-TSR TFC MANNHEIM GE//ASQE-OP-SCC//
MARCORCOMTELACT QUANTICO VA//
NAVCOMTELSTA SAN DIEGO CA//
NTCC CAMP H M SMITH HI//
DISA WASHINGTON DC//COS/D2/D35/D36/D5/D6/D7/D8//
DISA PAC WHEELER AAF HI//PC2/PC21/PC31//
DISA EUR VAIHINGEN GE//EU2/EU3/EU21//
DMC COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
DISA FLD OFC PETERSON AFB CO//JJJ//
DISA CENTRAL COMMAND FWD//JJJ//
DISA FLD OFC FT MCPHERSON GA//SANM//
DISA FIELD OFC NORFOLK VA//FAN//
DISA FLD OFC QUARRY HEIGHTS PM//
DISA DCO-NCR RESTON VA//JJJ//
DISA DCO-SCOTT SCOTT AFB IL//DRC//
DISA DCO-HUA FT HUACHUCA AZ//JJJ//

DISA CENTRAL COMMAND MACDILL AFB FL//
DISA-PAC ELMENDORF AFB AK//

UNCLAS
REQUEST WIDEST DISSEMINATION OF THIS MESSAGE TO YOUR SUBORDINATE ORGANIZATIONS//

MSGID/GEN ADMIN/D36/AUG/97//

SUBJ/GUIDANCE FOR COMPLYING WITH ASD(C3I) POLICY, 5 MAY 97, MANDATING USE OF DEFENSE INFORMATION SYSTEMS NETWORK (DISN) OR FTS COMMON USER TELECOMMUNICATIONS SERVICES//

NARR/1. OFFICE OF THE ASST SECRETARY OF DEFENSE FOR C3I ISSUED 5 MAY 97 POLICY MEMORANDUM TO CLARIFY AND REINFORCE EXISTING POLICY MEMORANDUM (4640-13 AND 4640-14) MANDATING DOD USE OF DISN COMMON-USER SERVICE AND FTS. MEMO DIRECTS DISA TO PUBLISH PROCEDURES AND CRITERIA FOR REVIEWING REQUESTS FOR EXCEPTION TO USE DISN AND FTS. THIS MESSAGE PROVIDES INTERIM GUIDANCE FOR COMPLYING WITH SAID POLICY.

2. IAW ASD(C3I) POLICY, ALL DOD LONG-HAUL TELECOMMUNICATIONS REQUIREMENTS WILL BE SATISFIED BY DOD COMMON-USER DISN OR BY FTS 2000/2001. LONG-HAUL TELECOMMUNICATION SERVICES ARE ANY AND ALL INTERSITE (ENTERING OR LEAVING CONFINES OF POST, CAMP, STATION, BASE, INSTALLATION HEADQUARTERS, OR FEDERAL BUILDING) VOICE, DATA, AND VIDEO SWITCHING AND TRANSMISSION SERVICES AND ASSOCIATE NETWORK MGMT, TO INCLUDE REGIONAL SERVICES, METROPOLITAN AREA NETWORKS (MANS), AND ASYNCHRONOUS TRANSFER MODE EDGE DEVICES.

3. EFFECTIVE IMMEDIATELY, ANY DOD LONG-HAUL NETWORK OR CIRCUIT (EXISTING, NEW, OR UPGRADE) MUST BE COMPLIANT WITH THIS POLICY. IF NOT COMPLIANT, YOU MUST SUBMIT TO DISA A REQUEST FOR EXCEPTION TO THE 5 MAY 97 POLICY. DISA, AS THE MANAGER/SOLE PROVIDER OF LONG-HAUL AND REGIONAL TELECOMMUNICATION SERVICES, WILL ASSESS YOUR REQUEST AND ISSUE A WAIVER TO POLICY. WAIVERS WILL BE GRANTED ONLY UNDER EXTRAORDINARY CIRCUMSTANCES WHERE AN INITIATIVE OR REQUIREMENT CANNOT AT THIS POINT IN TIME BE TECHNICALLY OR ECONOMICALLY SATISFIED BY DISN OR FTS.

4. SUBMIT REQUEST FOR EXCEPTION TO POLICY TO DISA D36, 701 COURTHOUSE ROAD, ARLINGTON, VA 22204-2199 OR EMAIL TO CENACJ@NCR.DISA.MIL. PROVIDE THE FOLLOWING INFORMATION:

A. REQUIREMENT/NAME/TYPE OF NETWORK OR SERVICE (NUMBER OF T1/3S FROM PORT A TO PORT B, ABCNET, SECRET, ATM NETWORK, OR XYZNET, UNCLAS MAN). PROVIDE CUSTOMER BASE, CONTRACT VEHICLE, AND GEOGRAPHIC LOCATION(S) SERVED. IDENTIFY PRINCIPAL USERS SUPPORTED.

B. JUSTIFICATION/NARRATIVE INCLUDING GENERAL DESCRIPTION OF THE REQUIREMENT/NETWORK OR SERVICE, THE PROPOSED SOLUTION, AND AN EXPLANATION AS TO WHY DISN OR FTS COMMON-USER SERVICE CANNOT BE USED.

C. SUMMARY OF PLANS TO MIGRATE TO DISN OR FTS COMMON-USER SERVICE.

D. POINT OF CONTACT - NAME, ORGANIZATION, PHONE, EMAIL AND MAILING ADDRESS.

5. UPON RECEIPT OF REQUEST FOR EXCEPTION, DISA WILL MAKE AN INDEPENDENT ASSESSMENT OF THE TECHNICAL AND ECONOMIC FEASIBILITY

FOR IMMEDIATE MIGRATION TO DISN OR FTS. DISA D36 WILL NOTIFY REQUESTING SERVICE/AGENCY WITHIN 30 DAYS OF ASSESSMENT RESULTS.

6. DISA POINT OF CONTACT IS MS JEAN CENAC, D36, (703) 735-8168 (DSN 653-8168), EMAIL: CENACJ@NCR.DISA.MIL.//

NOTE POC FOR WAIVERS AS BEEN CHANGED TO MS BETTY LEWIS AT 703-735-8168 (DSN) 653-8168, EMAIL: D3WAIVE@NCR.DISA.MIL

16. PREMISE ROUTER MANAGEMENT

A. The RCC will perform remote customer premise management for CISCO or Wellfleet routers connected directly to the SIPRNET. The fee for this service is $50.00 per month, per router. This service will be obtained via submission of a Telecommunications Service Request (TSR). The customer must include in line item 401 of the TSR request for this service, ie: Request DISA provide customer premise management of CISCO/Wellfleet router located at.....

B. Premise router management will only extend to the premise router equipment connected directly to a SIPRNET Hub router. Premise router management will not extend beyond the first premise router. This means access circuits beyond the customer premise router will not be managed as part of this service offering.

C. Network management services will consist of the following.

1. Router configuration table management, to include updating and reloading, activating protocols, configuring routers, and addressing. Note, DISA will provide initial configuration of customer premise routers, for those routers that can be configured remotely.

2. Remote fault isolation and troubleshooting of the customer premise router.

3. Restoration service, across the network, of hardware equipment and software configuration. Premise router maintenance is NOT included in this service offering.

D. It is the customers responsibility to ensure the DISA RCC receives router updates to their router configuration requirements and all premise router passwords necessary for network/configuration management. The customer must be able to provide on site personnel, at the customer premise, to aid in remote fault isolation and troubleshooting. The DISA RCC is the only authorized agent to make premise router configuration changes. Therefore, only the RCC will have the second level password.

17. DIAL UP CONNECTIVITY

For those customers who do not feel they have a direct SIPRNET requirement and wish to utilize the dial up offering this can be obtained by contacting the SIPRNET Support Center. 1-800-582-2567 / 703-821-6260. It must be understood by the customer that the monthly recurring fee for dial up access is per access card and not per site.

SIPRNET

(INITIAL MODELING REQUEST)

INFORMATION REQUIRED TO OBTAIN B SIDE INFORMATION

SYSTEM NAME______________________________________
(Not SIPRNET)
CONTRACTOR Facility _____ **YES**_______**NO**_______
ASSOCIATED SERVICE/SPONSOR ____________________________
(Army, Air Force, Navy, Specific Agency)
REQUIRED OPERATIONAL DATE______________________________
(Based on minimum lead time of **120** Days from TSR Receipt by his office)
SPEED___________
BUILDING___________________
ROOM_________
SPECIFIC MAILING ADDRESS______________________________
____
EQUIPMENT_____________________
(That which is connecting directly to SIPRNET HUB router)
POC____
(At host connection location, not Headquarters)
PHONE (comm)_____________________**(dsn)**____________________
USERs ORGANIZATION____________________________________
SITE COMM PERSONNEL___________________________________
(ie: Base Comm Office, if available)
PDC____
(Program Designator Code) (If this is not immediately available place To Be Determined on form. It is not critical at this point but must be included in RFS/TSR)

INFORMATION PAPER

Subject: Access Policy for Allies on the Secret Internet Protocol Router Network (SIPRNET)

Purpose. To provide information on the access policy and process for connecting allies to the SIPRNET

Major Points

Access Policy

SIPRNET is a Secret, US-only network. However, connections to agencies of foreign governments are permissible through the use of approved security devices employed on each foreign connection to the SIPRNET. These security devices must be in US controlled spaces.

The 7 Nov 95 MCEB approved the access approval process for allies on the SIPRNET

Access Approval Process

The CINC, as the sponsoring activity for the foreign connection, must first request Joint Staff/J6 approval of the requirement in accordance with CJCSI 6211.02A.

Joint Staff/J6 validates the requirement and forwards the request to DISA/D3 (Data Network Support Division) to work a technical solution.

The technical solution is worked jointly with the DISN Security Accreditation Working Group (DSAWG), DISA/D3, and CINC representatives. Additional technical expertise and assistance may be requested from NSA and the Joint Interoperability and Engineering Organization, as required.

After a technical solution has been decided, the solution is presented to the DSAWG for approval. If approved by the DISN Designated Approving Authorities (DAAs), which include the Joint Staff, DIA, NSA, and DISA, the DSAWG will advise both the sponsoring CINC and DISA/D3 in writing.

The CINC coordinates with the SIPRNET project office in DISA/D3 to complete the SIPRNET connection.

J6 Point of Contact: Gary Klabunde, Major
J6T, J-6 703-697-7091

Prepared by: Tina M. Harvey, Major, USAF
J6T, J-6, 693-1747

-- SAMPLE RFS --

FM DISA WASHINGTON DC//D343//
TO (Your appropriate TCO support, DCO-SCOTT, DCO-NCR, etc;)
INFO DISA WASHINGTON DC//D343/D345//

MESSAGE ADDRESSES OF STATIONS AT THE USER LOCATION AND WITHIN YOUR COMMAND/AGENCY WHO WILL HAVE TO TAKE ACTION ON THIS RFS

***NOTE: (P) = PERMANENT, THE INFORMATION CONTAINED IN THESE ITEMS SHOULD ALWAYS BE THE SAME. PLEASE ENSURE THAT YOU REMOVE ALL THE (P) BEFORE YOU SUBMIT YOUR RFS.

BT
UNCLAS
SUBJ: REQUEST FOR SERVICE
A. TSRE (DATADCS, LEASED, INTRA CONUS, DISN)
101. DATE AND YOUR RFS NUMBER (ie; RFS27FEB980001/2/3 etc;)
102. TSP # (Required if a CHANGE, AMEND or DISCONTINUE.
103. START (P) (Type action, START, CHANGE, Amend etc.)
104. CIRCUIT ONLY/SINGLE VENDOR - (P)
105. DISN ROUTER SERVICE - (P)
106A. 160001Z JAN 97 (DATE YOU WANT SERVICE) - (P)
106B. 160001Z JAN 97 (DATE YOU WANT SERVICE) - (P)
108. S7 - (P) (Purpose and use code)
109. 4G - (P) FOR 1.544MB, 4F FOR 0-64KB, 5A FOR 64KB TO 768KB, NS FOR 10MB
110. FULL DUPLEX - (P)
111. SPEED OF SERVICE YOU WANT, IE 64KB, 128KB, 512KB, 1.544KB
112. FULL PERIOD (P)
115. NO SIGNALING - (P)
116. NEW LEASE - (P)
117. YOUR PDC CODE
118. AMOUNT OF MONEY FOR OVERTIME AND EXPEDITE IF YOUR REQUEST IS UNDER 120 DAYS. (This only for payment of extra funds to commercial vendor.
Normal connections with the appropriate lead times do not require this field.)
119D. YES/ALL SATELLITE - (P) (Transmission media to be avoided) (If YES, Item #408 is required)
120A. FALCON (User location) GEOLOCO IF AVAILABLE
121A. 08 (State / Country code) IF KNOWN
122A. 1 (Area Code) IF KNOWN
123A. SPH-(P) (Facility Code) (SPH = SIPRNET Host / GCH = GCCS Host)
124A. BUILDING (To include street address)
125A. ROOM
126A. CISCO (ROUTER SERIES NUMBER, IE: 7500, 7000, ETC
127A. KIV-7HS
128A. DISA TO PROVIDE CSU/DSU. INTERFACE RS-530, V.35 etc. - (P)
129A. 4W-(P)
130A. USER POC NAME AND BOTH COMMERCIAL AND DSN PHONE NUMBERS. ONE ALTERNATE NAME AND PHONE NUMBER.
131A. COMPLETE ADDRESS (For user) (Mailing Address)
139A. NPANNX example: 703-735-3238 = my phone number
NPANNX = 703735

(There would be no break here. Only for this SAMPLE. B information will be provided by DISA D3113)
Once TSO is issued RFS must contain both "A" & "B" location information.

120B. HUB ROUTER LOCATION
121B. STATE/COUNTRY CODE
122B. SEE 122A
123B. SP1 - (P)
124B. BUILDING NUMBER (Where SIPRNET Hub is located)
125B. ROOM NUMBER
126B. TYPE OF TERMINAL EQUIPMENT
127B. KIV-7HS

128B. DISA TO PROVIDE CSU/DSU. INTERFACE RS-530 - (P)
129B. 4W - (P)
130B. HUB ROUTER POC NAME AND BOTH COMMERCIAL AND DSN PHONE NUMBERS. ALTERNATE NAME AND PHONE NUMBERS.
131B. COMPLETE ADDRESS (Mailing)
139B. AREA CODE/FIRST THREE NUMBERS OF PHONE NUMBER
353. SYSTEM ACRONYM – SYSTEM/PROJECT NAME
363. COMSEC ACCOUNT NUMBER
364. COMSEC CUSTODIAN - COMMERCIAL/DSN PHONE NUMBER
365. COMSEC CUSTODIAN MAILING ADDRESS
366. COMSEC CUSTODIAN PLA (Autodin) ADDRESS
401. RFS ISSUED TO PROVIDE, INSTALL, MAINTAIN A (SPEED OF CIRCUIT) CIRCUIT AND ASSOCIATED GFE EQUIPMENT BETWEEN SERVICE POINTS INDICATED, ALSO TO ESTABLISH TSP.
402. POC: YOUR NAME, ORGANIZATION, AND PHONE NUMBERS.
403. Y3 - (P)
408. JUSTIFICATION FOR SATELLITE OR OTHER EXCLUSION IDENTIFIED IN ITEM 119D.
410. COMMERCIAL VENDOR/TELCO BLDG/ROOM DEMARC POINT LOCATION TO INCLUDE STREET ADDRESS AND POC/PHONE NUMBER.
415B. SIPRNET
417. A. IF YOU HAVE ANY SPECIAL INSTALLATION REQUIREMENTS YOU WILL LIST THEM HERE. PLEASE INCLUDE YOUR SPECIFIC NAME WITHIN THIS BLOCK.

B. THE CIRCUIT VENDOR WILL TELEPHONICALLY CONTACT THE SITE POCs A MINIMUM OF 24 HOURS PRIOR TO ANY ONSITE INSTALLATION ACTIONS.

C. IF THE VENDOR IS UNABLE TO CONTACT SITE PERSONNEL CONTACT (YOUR NAME AND PHONE NUMBERS)

D. AUTHORIZATION FOR UTILIZATION OF THIS PDC IS AGAIN YOUR BOSS's NAME, ORGANIZATION, PHONE NUMBER. (HIS/HER SIGNATURE BLOCK)

E. THIS REQUIREMENT IS IN SUPPORT OF THE CLASSIFIED SIPRNET ROUTER NETWORK.

F. RFS POC: YOUR NAME AND PHONE NUMBERS

430. 60 MONTHS - (P) (How long do you need the connection? Normally not done longer than 60 or less than 12 months)
431. D - (P)
437A. CPIWI - (Yes/No) CPIWM - (Yes/No) (Do you want vendor to install and maintain the local circuit path from the commercial demarc to your location) (If yes, item 410A will be commercal demarc location.
437B. CPIWI - CPIWM -
438A. NONE - (P) (Leased equipment requirement)
438B. NONE - (P) (Leased equipment requirement)
440A. WILL NOT LEAK - CAT 6 - (P)
440B. WILL NOT LEAK - CAT 6 - (P)
444. INTERSTATE USE, 100 PERCENT - (P)
BT

If you require TSP line items 521, 525, 526A, B, and C, 529, and 531 are required. Refer to DISA Cir 310 130-1 page 3-58.

GLOSSARY:

SIPRNET-	Secret Internet Protocol Router Network
POC-	Point Of Contact
RFS-	Request For Service
TSR-	Telecommunications Service Request
TSO-	Telecommunications Service Order
TCO	Telecommunications Certification Office
CSU/DSU	Channel Service Unit/Digital Service Unit ie: modem
FE	Field Engineer
DOD	Department of Defense
DSS	Defense Security Service
SIPRNIC	Secret Internet Protocol Router Network Information Center
GFE	Government Furnished Equipment
RCC	Regional Control Center
PLA	Plain Language Address
Premise Routers	These are customer owned equipments not to be confused with Hub equipments which are actually part of the SIPRNET.
Backside Connections	Those connections to premise equipments. Not to actual SIPRNET Hub.
PDC	Program Designator Code - Funding code. This is between 4 and 6 characters and is how DISA is paid for connections to the SIPRNET.
DEMARC	This is that point where commercial vendors terminate their connections at a particular facility. A phone closet, DCO (Dial Central Office) etc.
IATC	Interim Approval To Connect
IATO	Interim Approval to Operate
DAA	Designated Approving Authority

SECURITY PACKAGE INFORMATION

1. Customer is required to complete the Security Accreditation documentation and return to D3124. They must also understand that this is parallel with other efforts to be completed for connectivity. The specific POC within D3124 for security package information is as follows:

Any questions regarding Security Packages and their requirements should be addressed to: Mr. John Staples 703-735-3236, (d) 653-3236. STAPLESJ@NCR.DISA.MIL

Mailing Address for Security Accreditation Package:

Defense Information Systems Agency
Code D3124
ATTN: Mr. Joseph Boyd
11440 Isaac Newton Square
Reston, Virginia. 20190-5006

A. Package will consist of the following as the Security Checklist for Interim Approval to connect to the SIPRNET.

1. Evidence of Risk Acceptance by cognizant authority.

a. An Accreditation letter or Interim Approval to Operate (IATO) signed by the DAA.

1. This letter should state the following:

a. The System

b. Mode of Operation
1. System High
2. Dedicated
3. Multi Level
4. Periods Processing

c. Maximum level of sensitivity of information processed.
1. Unclassified (U)
2. Sensitive but Unclassified (N)
3. Confidential (C)
4. Secret (S)
5. Top Secret (TS)

d. Statement of the Residual/Significant Risk assumed by the DAA.

1. This is a summary of the results of a risk assessment.
2. This to include risks presented by connected networks/systems

2. Statement of Minimum Security Requirements

a. Security Policy
b. System Security Plan

3. Statement of Specific Security Features and Implementation.

a. Concept of Operations
b. Security Concept of Operations
c. Security Standard Operating Procedures

4. System Connectivity Drawing/Configuration/Topology

a. Indicate connection to SIPRNET
b. Show connections to other networks/systems
c. Show proposed connections to other networks/systems

5. Provide MOAs/MOUs/Letters of Agreement of all connections to other networks/systems.

a. Identify connections to NON-DOD networks/systems

6. Consent to DISA Monitoring statement per DISA message DTG 121713 DEC 95. Subject DISN SIPRNET Interim Network Connection Requirements.

7. System Identification

   a. IP Address of premise router
   b. List Authorized, (SIPRNET REGISTERED), Class B and Class C licenses

8. Security Checklist / SIPRNET Access Assessment – See forms further in document.

CONTRACTOR FACILITY CONNECTIONS / SECURITY PROCESS

A. Contractor facility connections vary somewhat from those connections for DOD Service or Agencies.

1. Sponsor contacts J6 for validation of requirement.

2. J6 sends approval to D3124 / Mr. John Staples

3. D3124 sends copy of approval to DSS / Mr. Larry Moore along with name and number of customer and sponsor.

4. DSS contacts customer and DSS Field Office for action/IATO. Field Office involved determined by geographical location of customer requirement.

a. Security Package submitted by DSS (Field Office) based on information received from customer.

b. IP Addresses determined by DSS Field Representative and sent to Mr. Larry Moore at DSS Headquarters.

5. Full Security package sent from DSS to D3124.

6. D3124 sends Security package to IPMO

7. IPMO issues Interim Approval TO Connect (IATC).

8. Customer Connects to SIPRNET.

Checklist for SIPRNet Connection

*Package # ___________
*CCSD # ___________

1. Evidence of Risk Acceptance by cognizant authority:

___ Accreditation by DAA (Maximum of Three Years) Expiration: ___________
___ Interim Approval To Operate (Maximum of One Year) Expiration: ___________
(must include Statement of Residual/Significant Risk)

2. System Connectivity Drawing/Configuration/Topology
(to include backside connections, IP addresses, Encryption Devices)

3. Consent to DISA Monitoring...
Online verification of conformance with security information

4. SIPRNet Access Assessment Form (Must be included in initial package)
____Yes: 1 2 3 4 5 6 7 8 9 (circle applicable numbers) ____All No

5. Statement of Minimum Security Requirements (must have at least one):
___ System Security Policy
___ System Security Plan ___ Other (specify)______________________________

6. Statement of Specific Security Features and Implementation (must have at least one):
___Concept of Operations ___Security Standard Operating Procedures
___Security CONOPS ___Other (specify)

7. Copies of any other external connections and/or associated operational agreements:
___MOAs/MOUs ___Letters of Agreement
___Not Applicable

8. Mode of Operations:
___System High
___Dedicated
___Multi Level

9. Maximum level of sensitivity of information processed:
___Unclassified
___Unclassified but Sensitive
___Confidential
___Secret
___Top Secret

10. IP Registration: ________________________ ____Yes ____No

NOTE: Items 1-4 are mandatory requirements to obtain the Interim Approval to Connect (IATC).

SIPRNet Access Assessment

Reference or DISA Package Number: ______________________________
Command Communications Service Designator (CCSD): ______________________________
Organization (CINC / Service / Agency / Contractor Name): ______________________________
Location: ______________________________
Date ______________________________
Plain Language Address (PLA)(Government Only): ______________________________
POC and Phone number: ______________________________
System or Network Name: ______________________________
Premise Router IP Address: ______________________________
Network IP Address Ranges: ____________ ____________ ____________
____________ ____________ ____________ ____________

This form is to be submitted with the initial request for connection and exercises. Additionally, this form is to be re-accomplished when there is a change to the approved configuration, recertification, or a change that affects the answers on file.

Foreign National Access

#1 Yes No Foreign nationals, to include Integrated Officers (Foreign nationals in US positions), **have physical access to areas** where workstations **connect directly or indirectly** to the SIPRNet.
(Example: If other than US personnel have access (escorted or unescorted) to the SIPRNet workstation areas, a Yes response is required.)

#2 Yes No Foreign nationals, to include Integrated Officers, are **users** on workstations on a network or subnet **connected directly or indirectly** to the SIPRNet.
(Example: If other than US personnel have user accounts on SIPRNet workstations, a Yes response is required.)

#3 Yes No Foreign nationals, to include Integrated Officers, are **users** on workstations on a **separate network connected directly or indirectly** to SIPRNet.
(Example: A Non US network connected to a SIPRNet connection or using SIPRNet backbone as a transport layer to another Non US network, a Yes response is required.)

Contractor Access

#4 Yes No Uncleared contractors **have physical access to areas** where workstations on the organization network o its subnets **connected directly or indirectly** to the SIPRNet.
(Example: Uncleared contractor personnel, either in support of a Government contract or maintenance support, to include cleaning people, have access to SIPRNet workstations, a Yes response is required)

#5 Yes No Uncleared contractors are **users** on workstations **connected directly or indirectly** to the SIPRNet.
(Example: Any contractor (Prime or Sub), US or Non-US, having a user account on the SIPRNet, a Yes response is required. Explain if the contractor is located within an U.S. Government, non-U.S. Government or Contractor facility.)

#6 Yes No Cleared contractors at a non-DoD facility are **users** on workstations **connected directly or indirectly** t the SIPRNet. Contract Number(s): ______________________.
(Example: Any contractor (Prime or Sub) at a non-DoD facility (including Contractor facilities) on a separate network such as an Educational Facility, a Yes response is required.)

#7 Yes No Reference question #6. Are there any uncleared personnel providing support under this contract.
(Example: Any contractor personnel (Prime or Sub) that are providing administrative, logistical or services in support of the contract identified in numbe 6, a Yes response is required.

Network Connectivity - **Include the Secret and Below Interoperability (SABI) Ticket Number (if Applicable) :** __________

#8 Yes No The Organizational network, to include subnet(s) and workstation(s), connects to a network operating a any level other than US Only Secret either **with or without a high assurance guard** in place.
(Example: A network operating at Unclassified But Sensitive, Unclassified, Confidential, Top Secret, NATO Secret, etc., a Yes response is required.)

SIPRNet Access Assessment

If any of the above statements were answered with a **"YES"**, provide a **detailed** description of the systems involved, the security controls employed, information shared, allowed accesses, number of

foreign nationals, etc. and identify the Designated Approval Authority for that connection. Please be sure to sign and include the reference number on any and all attachments. Any questions may be directed to DISA, INFOSEC Program Management Office, Sonia Martinez at (703) 681-7957/9065, DSN 761-7957/9065 or email **martin5s@ncr.disa.mil.**

If this document and its attachments are classified after completion, please call the SIPRNet Connection Approval Office at DSN 761-7956/7966 to coordinate a secure fax transmittal. You may also return it by registered mail to the following address:

Defense Information Systems Agency
5113 Leesburg Pike, Suite 400
Falls Church, VA 22041
Attention: Sonia Martinez

If the document and its attachments are unclassified after completion you may fax it to COMM (703) 681-5756 or DSN 761-5756.

CERTIFICATION: I certify that the information provided in this document and all attachments are accurate.

OR

Signature Block
Designated Approving Authority (DAA)

Signature Block
Information System Security Officer
(ISSO)

<u>**DSS Addresses / Phone numbers**</u>

Northeast Region, DSS
New England Sector
Barnes Building 1040
495 Summer Street
Boston, Ma 02210-2192
COMM: (617) 451-4914
DSN: 955-4914
FAX: (617) 451-3052/4929

Northeast Region, DSS
Mid-Atlantic Sector
Kings Highway North
Cherry Hill, NJ 08034-1908
COMM: (609) 482-6505
DSN: 444-4030
FAX: (609) 482-0286

Central Region, DSS
Southwest Sector
106 Decker Court, Suite 200
Irving, TX 75062-2795
COMM: (214) 717-5228
FAX: (214) 717-0268

Central Region, DSS
Midwest Sector
610 S. Canal Street
Room 908
Chicago, IL 60607-4599
COMM: (312) 886-2436
FAX: (312) 353-1538

Pacific Region, DSS
Southern Sector
3605 Long Beach BLVD, Suite 405
Long Beach, CA 90807-4013
COMM: (310-595-7251
FAX: (310) 595-5584

Pacific Region, DSS
Northern Sector
Building 35, Room 114
The Presidio
San Francisco, CA 94129-7700
COMM:(415) 561-5608
FAX: (415) 561-2125

Capital Area, DSS
Hoffman Building
2461 Eisenhower Avenue
Alexandria, VA 22331-1000
COMM: (703) 325-9634
DSN: 221-9634
FAX: (703) 325-0792

Southeast Region, DSS
2300 Lake Park Drive
Suite 250
Smyrna, GA 30080-7606
COMM: (404) 432-0826
DSN: (697-6785
FAX: (404) 801-3300

MESSAGES RELATING TO SIPRNET SECURITY PACKAGES

UNCLASSIFIED

ROUTINE CHANNEL NO. 318992 04-22-96

RCTUZDKW RUEJDCA2712 1131812 MTMS-UUXX—XXXXXXX.1131822 318992 04-22-96
ZNR UUUXX
R 121713 DEC 95
FM DISA WASHINGTON DC//D343//
TO CONUSMILNETSTA
CONUSDSNET1STA
AIG 8787
AIG 8791
RUENAAA/CNO WASHINGTON DC//N6/N61/N62/N643//
RUEACMC/CMC WASHINGTON DC//C4I/CS/CCT//
RUEAHQA/HQ USAF WASHINGTON DC//SC/SCM/AQPC//
RUEADWD/DA WASHINGTON DC // DISC4/SAIS-ADM/DAMO-FD//
INFO RUEKJCS/SECDEF WASHINGTON DC//OASD:C3I//
RUEKJCS/JOINT STAFF WASHINGTON DC//J3/J6/J6S/J6T/J6V/J6Z//
RUEOFFA/ESC HANSCOM AFB MA//AVN//
RHCUABA/HQ AFC4A SCOTT AFB IL//XPR//
RUEANBA/PM AWIS FT BELVOIR VA//SFAE-CC-AWT//
RUFTDCA/DISA EUR VAIHINGEN GE//EU/EU2/EU21//
RUHHAAA/DISA PAC WHEELER AAF HI//PC/PC2/PCC//
RUEOBSA/DISA CENTRAL COMMAND FWD//JJJ//
RUCJICD/DISA CENTRAL COMMAND MACDILL AFB FL//DF//
RUEAHUA/CDRUSAISC FT HUACHUCA AZ//ASOP//
RUVOBTA/HQ SSC MAXWELL AFB GUNTER ANNEX AL//SI/SIN/SSDN//
RULSWCB/COMNAVCOMTELCOM WASHINGTON DC//N13/N9/N7/N5//
RUETIAA/DIRNSA FT GEORGE G MEADE MD//Q11/Q21/Y414/Y441//
RUETICO/NSACSSTCO TSR TSO TRAFFIC FT GEORGE G MEADE MD//Q214//
RUET1AA/NSACSS FORT GEORGE G MEADE MD//Y443//
RUEOASI/ISPO ANNAPOLIS JUNCTION MD//JJJ//
RULSJGA/COGARD TISCOM ALEXANDRIA VA//CPD/OPS-3//
RULSJGA/COMDT COGARD WASHINGTON DC//G-OIN/G-TTM//
RUEADNA/DNA WASHINGTON DC//COMP-1/NOCC//
RUEANLA/DLA FT BELVOIR VA//CANAI//
RUDIDLJ/DSDC COLUMBUS OH//DDSAC-RBB/DOWCA//
RUEKJCS/JOINT STAFF WASHINGTON DC//J6T/J8//
RUCJACC/USCINCCENT MACDILL AFB FL//J6//
RUCJAAA/USSOCOM MACDILL AFB FL//J6//
RHHMUNA/USCINCPAC HONOLULU HI//J6//
RUCEAAA/HQ USSPACECOM CHEYENNE MOUNTAIN AS CO//J6//
RUCUSTR/USSTRATCOM OFFUTT AFB NE//J6//

UNCLASSIFIED

RHCUAAA/USTRANSCOM SCOTT AFB IL//J6//
ACTION D322 ADDR BY: 31 INTERNALLY GENERATED DISTRIBUTION COPY
INFO D6-JE D331 D31 DO WEY WE34 D2 D23 JEE JEJ JEX D21 D3 D333 D8 ISB JEB
THIS MESSAGE IS A RETRANSMISSION
RUEJDCA 2712 121713Z DEC 95
RHLBAAA/HQ SOUTHCOM QUARRY HEIGHTS PM//J6//
RUCBACM/USACOM NORFOLK VA//J6//
RUSNNOA/USCINCEUR VAIHINGEN GE//J6//
RUEASRB/CDRFORSCOM FT MCPHERSON GA//AFIS-O//
RUDHDMH/HQ DMA FAIRFAX VA//TSCEID//
RUEKJCS/DMSSC WASHINGTON DC//EIT/TCO//
RHCUAAA/DITCO SCOTT AFB IL//DTS//
RUWTSGT/DISA TMSO TSR-TSO-CRP TRAFFIC SCOTT AFB IL//QTN
RHCUABA/DISA SCOTT AFB IL//UNR/UNRSE/UNRSO//
RUEKDIA/DIA WASHINGTON DC//SC/SY/SY-3A/SY-3C//
RULSGAE/NAVCOMTELSTA WASHINGTON DC//N912//
RUCTPOL/NAVCOMTELSTA PENSACOLA FL//N51/N32//
RUEBAFA/JSC ANNAPOLIS MD//INS//
RUEARNG/ARNGRC ARLINGTON VA//NGB-AIS-SC//
RHDJAAA/CDR ANG SUPPORT CENTER ANDREWS AFB MD//ANGSC/SI//
RUDIZA/DMC RFS-TSR TRAFFIC DENVER CO//JJJ//
RUDIDFE/DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//TB/DFAS-IN-MI//
RUERFCP/CDRUSAISC COROZAL PM//ASNP-OPS//
RUDIDSA/DISA COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
RUWTNOK/DISA FLD OFC PETERSON AFB CO//JJJ//
RUEASRA/DISA FLD OFC FT MCPHERSON GA//SANM//
RUEOBSA/DISA CENTRAL COMMAND FWD DHAHRAN SA//JJJ//
RUCBSAA/DISA FLD OFC NORFOLK VA//FAN//
RHLBAAU/DISA FLD OFC QUARRY HEIGHTS PM//
RULSWCD/DISA DCO-NCR RESTON VA//JJJ//
RHCUABA/DISA DCO-SCOTT SCOTT AFB IL//DRC//
RUEAHUT/DISA DCO-HUA RFS-TSR TRAFFIC FT HUACHUCA AZ//JJJ//
RUEJDCA/DISA WASHINGTON DC//ISB/ISBE/ISBG/ISBGC/D2/D21/D3/D34/D343/D381
/JE/JT/WE/WEZ51/WE312//
BT
UNCLAS
OPER/CONUSMILNETSTA 06/95/CONUSDSNET1STA 04/95/ZDK RETRANSMISSION
DUE TO NUMEROUS REQUESTS/REF DISA D343/182100Z APR 96//
SUBJ/DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET)
INTERIM NETWORK CONNECTION REQUIREMENTS//
REF/A/DOC/CJCSI 6211.02, DEFENSE INFORMATION SYSTEM NETWORK AND
CONNECTED SYSTEMS, 23 JUN 93//
REF/B/DOC/CJCS MOP 43, MILITARY TELECOMMUNICATIONS AGREEMENTS AND

ARRANGEMENTS BETWEEN THE UNITED STATES AND REGIONAL DEFENSE ORGANIZATIONS OR FRIENDLY FOREIGN NATIONS, 11 MAR 92// POC/JOSEPH BOYD/GS/D34/LOC:DISA WASH/TEL:DSN 653-8290/TEL:COMM (7030735-8290//

RMKS/1. IAW REFERENCE A, CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION, ENCLOSURE B, PARA. 3.J., DISA WILL "ESTABLISH AND PUBLISH DISN CONNECTION REQUIREMENTS, IDENTIFICATION AND ACCREDITATION PROCEDURES, AND PUBLISH TO THE UNITED AND SPECIFIED COMMANDS, SERVICES, AND DEFENSE AGENCIES." DISA IS CURRENTLY IN THE PROCESS OF WRITING THE CONNECTION REQUIREMENTS FOR THE DEFENSE INFORMATION INFRASTRUCTURE (DII). DISA IS COMMITTED TO ENSURING THE PROTECTION OF THE DII AND PROVIDING INFORMATION SYSTEMS SERVICES TO THE WARFIGHTER. THE PURPOSE OF THIS MESSAGE IS TO PROVIDE EXISTING AND POTENTIAL SIPRNET SUBSCRIBERS WITH CONNECTION REQUIREMENTS THAT MUST BE FOLLOWED UNTIL THE DII REQUIREMENTS ARE PROMULGATED (ESTIMATED $2^{ND}/3^{RD}$ QTR FY96). THE DII CONNECTION REQUIREMENTS WILL IDENTIFY SECURITY REQUIREMENTS AND PROHIBITIVE ACTIONS REGARDING SIPRNET NETWORK ACCESS.

2. THE FOLLOWING REQUIREMENTS MUST BE MET BEFORE A NEW CONNECTION TO THE SIPRNET IS GRANTED.

A. CONTACT SIPRNET PROJECT OFFICE: AL CONUS CUSTOMERS DESIRING A DIRECT CONNECTION TO THE SIPRNET MUST FIRST MAKE CONTACT WITH THE PROJECT OFFICE, DISA/D343. PLEASE CONTACT MR. JOSEPH BOYD (SIPRNET PROJECT MANAGER) AT (703) 735-8290 (DSN 653-8290) OR MR. JIM NOSTRANT AT (703) 735-3238. EUROPE CUSTOMERS ARE TO CONTACT MR. BOB MAULDIN, DISA-EUR, AT DSN 314-430-8457. PACIFIC CUSTOMERS ARE TO CONTACT MR. LESTER PANG, DISA-PAC, AT DSN 315-456-2858.

B. SYSTEM SECURITY PACKAGE: IN ORDER FOR DISA TO APPROVE CONNECTIVITY TO SIPRNET, ALL AUTOMATED INFORMATION SYSTEMS (ais) CURRENTLY CONNECTED OR DESIRING CONNECTIVITY MUST SUBMIT THE BELOW LISTED DOCUMENTATION TO THE DEFENSE INFORMATION SYSTEMS AGENCY, ATTN: D343 (JOSEPH BOYD), 11440 ISAAC NEWTON SQUARE, RESTON VA 22090-5087

- ACCREDITATION LETTER. SIGNED BY THE COGNIZANT DESIGNATED APPROVAL AUTHORITY (DAA) FOR THE NETWORK/SYSTEM REQUIRING SIPRNET CONNECTION. IF THE AIS IS NOT ACCREDITED, INDICATE IF SYSTEM IS OPERATING UNDER AN INTERIM APPROVAL TO OPERATE (IATO). THE SIPRNET CONNECTION WILL NOT BE GRANTED UNLESS EVIDENCE OF AN ACCREDITATION OR IATO IS PROVIDED.
- INTERIM APPROVAL TO OPERATE. IF AN IATO HAS BEEN GRANTED, ADVISE THIS OFFICE OF ALL SIGNIFICANT RISKS THE SYSTEM IS CURRENTLY OPERATING UNDER. SIGNIFICANT RISKS INCLUDE LACK OF IDENTIFICATION

AND AUTHENTICATION MECHANISMS, LACK OF AUDIT FUNCTION, UNPROTECTED CONNECTIONS TO OTHER NETWORKS, UNAUTHENTICATED AND UNPROTECTED DIAL-IN CAPABILITIES, ETC.

- AIS CONCEPT OF OPERATIONS AND SECURITY POLICY OF EQUIVALENT DOCUMENTATION. THESE SECURITY DOCUMENTS WILL DESCRIBE HOW SECURITY REQUIREMENTS HAVE BEEN IMPLEMENTED IN THE ENVIRONMENT FURTHER, THESE DOCUMENTS WILL IDENTIFY DATA TYPES, CLASSIFICATION LEVEL OF DATA, SYSTEM OWNER, AND DESIGNATED APPROVING AUTHORITY.

- SYSTEM CONNECTIVITY DIAGRAM. THIS DIAGRAM SHALL IDENTIFY ALL AIS CONNECTIONS, BOTH FRONT AND BACKSIDE., TO INCLUDE ANY CONNECTIONS TO OTHER GATEWAYS DIRECTLY OR INDIRECTLY CONNECTED TO OTHER NETWORKS.

- FOREIGN CONNECTIONS. THE SIPRNET IS A "SECRET, SYSTEM HIGH, U.S. ONLY" NETWORK. HOWEVER, CONNECTIONS TO AGENCIES OF FOREIGN GOVERNMENTS MAY EXIST. ALL FOREIGN CONNECTIONS TO THE SIPRNET MUST FIRST BE VALIDATED BY THE JOINT STAFF (UNDER THE PROVISIONS OF REF B) AND APPROVED IN ACCORDANCE WITH THIS MESSAGE. ALL FOREIGN CONNECTIONS WILL REQUIRE THE INSTALLATION OS A HIGH ASSURANCE GUARD DEVICE OR AN END-TO-END ENCRYPTION DEVICE. BOTH TYPES OF DEVICES SHALL BE UNDER US CONTROL (PROCURED, OPERATED, MAINTAINED, AND CONFIGURED BY THE U.S. SPONSORING ACTIVITY) AND UTILIZED TO PREVENT UNAUTHORIZED OR ACCIDENTAL DISCLOSURE OF CLASSIFIED, U.S. ONLY INFORMATION ON THE SIPRNET.

- ACKNOWLEDGMENT OF PERIODIC MONITORING AND VULNERABILITY ASSESSMENTS. ALL CONNECTION REQUESTS MUST PROVIDE THE FOLLOWING STATEMENT: "WE ACKNOWLEDGE AND CONSENT TO DISA CONDUCTING AN INITIAL VULNERABILITY ASSESSMENT AND PERIODIC UNANNOUNCED VULNERABILITY ASSESSMENTS ON THE CONNECTED HOST SYSTEMS TO DETERMINE THE SECURITY FEATURES IN PLACE TO PROTECT AGAINST UNAUTHORIZED ACCESS OR ATTACK."

3. THE FOLLOWING REQUIREMENTS MUST BE MET FOR EXISTING SIPRNET CONNECTIONS. THE REQUIREMENTS IDENTIFIED IN PARA 2 APPLY. AN INTERIM APPROVAL TO CONNECT TO SIPRNET IS GRANTED FOR 90 DAYS FROM THE DTG OF THIS MESSAGE. WITHIN THIS TIMEFRAME, THE COGNIZANT SERVICE/ AGENCY MUST SUBMIT THE SYSTEM SECURITY PACKAGE WITHIN 90 DAYS OF THE DTG OF THIS MESSAGE. FOREIGN CONNECTIONS MUST BE IDENTIFIED, VALIDATED, AND APPROVED BY THE JOINT STAFF DURING THIS TIMEFRAME. FAILURE TO COMPLY MAY RESULT IN SERVICE DISRUPTION.

4. DISA RESERVES THE RIGHT TO DENY OR DISCONTINUE SIPRNET ACCESS TO RISK
ANY NETWORK OR SYSTEM DEMONSTRATING BEHAVIOR THAT INCREASES TO THE SIPRNET INFRASTRUCTURE AND TO SIPRNET SUBSCRIBERS.

5. THE DISN CERTIFICATION AUTHORITY (DISA CISS) WILL REVIEW THE ABOVE REQUESTED DOCUMENTATION AND MAKE A CONNECTION APPROVAL DETERMINATION. THE JOINT STAFF WILL VALIDATE AND APPROVE ALL FOREIGN CONNECTIONS. UPON REVIEW OF THE DOCUMENTATION PROVIDED AND INITIAL SECURITY CONCERNS ARE SATISFIED, THE CISS WILL ISSUE AN INTERIM APPROVAL TO CONNECT TO THE SIPRNET FOR A PERIOD OF 90 DAYS. THE FINAL APPROVAL TO CONNECT WILL BE PROVIDED BASED ON SUCCESSFUL COMPLETION OF THE VULNERABILITY ASSESSMENT AND SATISFACTION OF SECURITY DOCUMENTATION. SIPRNET REQUESTS FOR SERVICE AND FEEDER TSR'S CAN BE SUBMITTED CONCURRENT WITH THE ABOVE DOCUMENTATION; HOWEVER, CONNECTION ACTIVATION WILL NOT OCCUR UNTIL AN INTERIM CONNECTION APPROVAL IS GRANTED IN WRITING.
6. REQUEST DISA-EUROPE AND DISA-PACIFIC PROVIDE FURTHER DISSEMINATION OF THIS MESSAGE WITHIN YOUR RESPECTIVE THEATERS.
7. DISA POC IS MR JOSEPH BOYD, DSN 653-8290/COMM 703-735-8290.//
BT
RCTUZDKW RUEJDCA2712 1131812 0218-UUUU

Note** Item #7 changed to Mr John Staples (DSN) 653-3236 (Comm) 703-735-3236

RUTUZYUW REDJDCA2006 1092052 MTMS-UUXX—XXXXXXX.1092101 318591
R182100Z APR 96
FM DISA WASHINGTON DC//D3//
TO CONUSMILNETSTA
CONUSDSNET1STA
AIG 8787
AIG 8791
CNO WASHINGTON DC//N6/N61/N62/N643//
CMC WASHINGTON DC//C4I/CS/CCT//
HQ USAF WASHINGTON DC//SC/SCM/AQPC//
DA WASHINGTON DC//DISC4/SAIS-ADM/DAMO-FD//
INFO SECDEF WASHINGTON DC//OASD:C3I//
JOINT STAFF WASHINGTON DC//J3/J6/J6S/J6T/J6V/J6Z//
ESC HANSCOM AFB MA//AVN//
HQ AFC4A SCOTT AFB IL//XPR//
CDR PM AWIS-CCS FT BELVOIR VA//SFAE-CC-AWT//
DISA EUR VAIHINGEN GE//EU/EU2/EU21//
DISA PAC WHEELER AAF HI//PC/PC2/PCC//
DISA CENTRAL COMMAND FWD//JJJ//
DISA CENTRAL COMMAND MACDILL AFB FL//DF//
VDRUSAISC FT HUACHUCA AZ//ASOP//
HQ SSC MAXWELL AFB GUNTER ANNEX AL//SI/SIN/SSDN//
COMNAVCOMTELCOM WASHINGTON DC//N13/N9/N7/N5//
DIRNSA FT GEORGE G MEADE MD//Q11/Q21/Y414/Y441//
NSACSSTCO TSR TSO TRAFFIC FT GEORGE G MEADE MD//Q214//
NSACSS FORT GEORGE G MEADE MD//Y443//
ISPO ANNAPOLIS JUNCTION MD//JJJ//
COGARD TISCOM ALEXANDRIA VA//CPD/OPS-3//
COMDT COGARD WASHINGTON DC//G-OIN/G-TTM//
DNA WASHINGTON DC//COMP-1/NOCC//
DLA FT BELVOIR VA//CANAI//
DSDC COLUMBUS OH//DDSAC-RBB/DOWCA//
JOINT STAFF WASHINGTON DC//J6T/J8//
USCINCCENT MACDILL AFB FL//J6//
USSOCOM MACDILL AFB FL//J6//
USCINCPAC HONOLULU HI//J6//
HQ USSPACECOM CHEYENNE MOUNTAIN AS CO//J6//
USSTRATCOM OFFUTT AFB NE//J6//
USTRANSCOM SCOTT AFB IL//J6//
HQ SOUTHCOM QUARRY HEIGHTS PM//J6//

USACOM NORFOLK VA//J6//
USCINCEUR VAIHINGEN GE//J6//
CDRFORSCOM FT MCPHERSON GA//AFIS-O//
HQ DMA FAIRFAX VA//TSCEID.//
DMSSC WASHINGTON DC//EIT/TCO
DITCO SCOTT AFB IL//DTS//
DISA TMSO TSR-TSO-CRP TRAFFIC SCOTT AFB IL//QTN//
DISA SCOTT AFB IL//UNR/UNRSE/UNRSO//
DIA WASHINGTON DC//SC/SY/SY-3A/SY-3C//
NAVCOMTELSTA WASHINGTON DC//N912//
NAVCOMTELSTA PENSACOLA FL//N51/N32//
JSC ANNAPOLIS MD//INS//
ARNGRC ARLINGTON VA//NGB-AIS-SC//
CDR ANG SUPPORT CENTER ANDREWS AFB MD//ANGSC/SI//
DMC RFS-TSR TRAFFIC DENVER CO//JJJ//
DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//TB/DFAS-IN-MI//
CDRUSAISC COROZAL PM//ASNP-OPS//
DISA COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
DISA FLD OFC PETERSON AFB CO//JJJ//
DISA FLD OFC FT MCPHERSON GA//SANM//
DISA CENTRAL COMMAND FWD DHAHRAN SA//JJJ//
DISA FLD OFC NORFOLK VA//FAN//
DISA FLD OFC QUARRY HEIGHTS PM//
DISA DCO-NCR RESTON VA//JJJ//
DISA DCO-SCOTT SCOTT AFB IL//DRC//
DISA DCO-HUA RFS-TSR TRAFFIC FT HUACHUCA AZ//JJJ//
DISA WASHINGTON DC//ISB/ISBE/ISBG/ISBGC/D2/D21/D3/D34/D343/D381/D6/
JE/JT/WE/WEZ51/WE312//
BT
UNCLAS
OPER/CONUSMILNETSTA 03/96/CONUSDSNET1STA 02/96//
SUBJ/DEADLINE EXTENSION TO DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS//
REF/RMG/DISA WASHINGTON DC/D/121713Z DEC 95//
POC/KYRA JENKINS/RM1/D343/LOC:DISA WASH/TEL:DSN 653-8041/TEL:COMM (703)735-8041//
RMKS/1.REF MESSAGE OUTLINES CONNECTION REQUIREMENTS FOR EXISTING AND POTENTIAL SIPRNET SUBSCRIBERS. THESE REQUIREMENTS ARE CRUCIAL FOR ENSURING OVERALL NETWORK SECURITY INTEGRITY AND TO FACILITATE FINAL ACCREDITATION OF THE SIPRNET.

2. FOR ALL EXISTING SIPRNET CONNECTIONS: AN INTERIM APPROVAL TO CONNECT TO SIPRNET IS HEREBY EXTENDED UNTIL 31 JUL 1996, AT WHICH TIME ALL REQUIREMENTS OUTLINED IN REF MESSAGE MUST BE COMPLETED. THIS EXTENSION IS DUE TO A SUBSTANTIAL NUMBER OF CUSTOMERS WHO DID NOT RECEIVE DISA'S ORIGINAL MESSAGE.
3. ALL CURRENT AND PROSPECTIVE SIPRNET CUSTOMERS ARE TO SUBMIT A SYSTEM PACKAGE WITH REQUIRED DOCUMENTATION TO DEFENSE INFORMATION SYSTEMS AGENCY. ATTN: D343 (RM1 KYRA JENKINS), 11440 ISAAC NEWTON SQUARE, RESTON, VA 22090-5087. FAILURE TO COMPLY MAY RESULT IN SERVICE DISRUPTION OR DENIAL OF CONNECTION APPROVAL. TO FACILITATE PACKAGE PROCESSING. REQUEST CUSTOMEWRS INCLUDE THE ASSIGNED COMMAND AND CONTROL SERVICE DESIGNATOR (CCSD) OR IP ADDRESS FOR EACH SIPRNET CONNECTION UNDER THEIR RESPONSIBILITY.
4. RECIPIENTS ARE REQUESTED TO ENSURE WIDEST DISSEMINATION OF THIS MESSAGE.
5. DISA POC IS RM1 KYRA JENKINS, DSN 653-8041/COMM 703-735-8041/EMAIL: JENKINSK@NCR.DISA.MIL.//
BT

Note** Change reference to RM1 Jenkins to Mr. John Staples (DSN) 653-3236 (Comm) 703-735-3236

ROUTINE

R 161945Z APR 97

FM JOINT STAFF WASHINGTON DC//VJ6//

TO CINCUSACOM NORFOLK VA//J2/J3/J6//
USCINCCENT MACDILL AFB FL//CCJ2/CCJ3/CCJ6//
USCINCSOC MACDILL AFB FL//SOJ2/SOJ3/SOJ6//
USCINCPAC HONOLULU HI//J2/J3/J6//
USCINCSPACE PETERSON AFB CO//J2/J3/J6//
USSTRATCOM OFFUTT AFB NE//J2/J3/J6//
USCINCTRANS SCOTT AFB IL//TCJ2/TCJ3/TCJ6//
USCINCSO SCJ6 QUARRY HEIGHTS PM//SCJ2/SCJ3/SCJ6//
USCINCEUR VAIHINGEN GE//ECJ2/ECJ3/ECJ6//
CNO WASHINGTON DC//N6/N61/N62/N643/N2/N3//
CMC WASHINGTON DC//C4I/CS/PPO/POC//
HQ USAF WASHINGTON DC//SC/SCM//
SAF WASHINGTON DC//AQI/AQII/AQPC//
DA WASHINGTON DC//DISC4/SAIS-ADM/DAMO-FD//
OSI WASHINGTON DC//SO/DR/CC//
FINCEN VIENNA VA//
FLTINFOWARCEN NORFOLK VA//N6/N62//
NAVLANTMETOC DET KEFLAVIK IC//JJJ//
COMICEDEFOR KEFLAVIK IC//J6//
USCS BAY ST LOUIS MS//
AEDC ARNOLD AFB TN//IN//
123IS LITTLE ROCK AFB AR//IN//
AFMC CSO WPAFB OH//SCMF//
DET 2 696 IG WPAFB OH//RMC//
USCINCCENT MACDILL AFB FL//CCJ6-C//
DIA WASHINGTON DC//SY//
COMMARCORSYSCOM QUANTICO VA//NOC/PMICS//
COMDR FORSCOM FT MCPHERSON GA //AFIN-RD/AFIN-ID/
/AFIS-OP/AFZK-IMP//
HQ AFSPC PETERSON AFB CO//LGS//
NATIONAL DRUG INTELLIGENCE CENTER JOHNSON PA//
DEA HQS WASHINGTON DC//SIOM//
CDRUSACAA BETHESDA MD //CSCA-CST//
AFPCA WASHINGTON DC//GAC/OPSD//

BBN SYSTEMS & TECHNOLOGIES CAMBRIDGE MA//MS6/4D//
CDRCECOM FT MONMOUTH NJ //AMSEL-MI-I//
COGARD COMMSTA MIAMI FL//
NAVOCEANO STENNIS SPACE CENTER MS//N624//
DPAC ANDREWS AFB MD//CH//
18 ABNCORPS FT BRAGG NC//AFZA-GT-OCR//
CDRICORPS FT LEWIS WA//AFZH-OO//
CDRIIICORPS FT HOOD TX//G2/G3/G6//
CDRVCORPS FRANKFURT GE//G2/G3/G6//
621AMOS MCGUIRE AFB NJ //IN//
COMSCLANT BAYONNE NJ//N6/N65/N652//
FITCPAC SAN DIEGO CA//02//
RUEHBK/AMEMBASSY BANGKOK//DEA//
RUEHWN/AMEMBASSY BRIDGETOWN//DEA//
NAVCOMTELSTA PENSACOLA FL//N32//
CCGDSEVEN MIAMI FL//OC/OI//
DISA WASHINGTON DC//D64//
DNA WASHINGTON DC//NOCC//
COMNAVSPACECOM DAHLGREN VA//N621//
CDR1111THSIGBN FT RITCHIE MD//ASQY-SRP-S/ASQY-SRP-N//
COMNAVRESFOR NEW ORLEANS
LA//N321/WE337/WE345/WE3452.DB//
INFO SECDEF WASHINGTON DC//OASD:C3I//
JOINT STAFF WASHINGTON
DC//J3/J33/CSOD/J6/J6S/J6T/J6V/J6Z/J2//
ESC HANSCOM AFB MA//AVN//
HQ AFCA SCOTT AFB IL//SYNE/XPR//
CDR PM AWIS-CCSFT BELVOIR VA //SFAE-CC-AWT//
DISA EUR VAIHINGEN GE//EU/EU2/EU21//
DISA PAC WHEELER AAF HI//PC/PC2/PCC//
DISA CENTRAL COMMAND FWD//JJJ//
DISA CENTRAL COMMAND MACDILL AFB FL//DF//
CDRUSAISC FT HUACHUCA AZ//ASOP//
HQ SSC MAXWELL AFB GUNTER ANNEX AL//SI/SIN/SSDN//
COMNAVCOMTELCOM WASHINGTON DC//N13/N9/N7/N5//
DIRNSA FT GEORGE G MEADE MD //Q11/Q21/Y414/Y441//
NSACSSTCO TSR TSO TRAFFIC FT GEORGE G MEADE
MD//Q214//
NSACSS FORT GEORGE G MEADE MD//Y443//
ISPO ANNAPOLIS JUNCTION MD//JJJ//
COGARD TISCOM ALEXANDRIA VA//CPD/OPS-3//

COMDT COGARD WASHINGTON DC//G-OIN/G-TTM//
DNA WASHINGTON DC//COMP-1/NOCC//
DLA FT BELVOIR VA//CANAI//
DSDC COLUMBUS OH//DDSAC-RBB/DOWCA//
CDRFORSCOM FT MCPHERSON GA//AFIS-O//
HQ DMA FAIRFAX VA//TSCEID//
DMSSC WASHINGTON DC//EIT/TCO//
DITCO SCOTT AFB IL//DTS//
DISA TMSO TSR-TSO-CRP TRAFFIC SCOTT AFB IL//QTN//
DISA SCOTT AFB//UNR/UNRSE/UNRSO//
DIA WASHINGTON DC//SC/SY-3A/SY-3C//
NAVCOMTELSTA WASHINGTON DC//N912//
NAVCOMTELSTA PENSACOLA FL//N51/N32//
JSC ANNAPOLIS MD//INS//
ARNGRC ARLINGTON VA//NGB-AIS-SC//
CDR ANG SUPPORT CENTER ANDREWS AFB MD//ANGSC/SI//
DMC RFS-TSR TRAFFIC DENVER CO//JJJ//
DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//TB//
DFAS-INDIANAPOLIS CENTER INDIANAPOLIS IN//DFAS-IN-MI//
CDRUSAISC COROZAL PM//ASNP-OPS//
DISA COLUMBUS OH//WE3-UNRRB/UNR/UNRBA/CRCC//
DISA FLD OFC PETERSON AFB CO//JJJ//
DISA FLD OFC FT MCPHERSON GA//SANM//
DISA CENTRAL COMMAND FWD DHAHRAN SA//JJJ//
DISA FLD OFC NORFOLK VA//FAN//
DISA FLD OFC QUARRY HEIGHTS PM//
DISA DCO-NCR RESTON VA//JJJ//
DISA DCO-SCOTT SCOTT AFB IL//DRC//
DISA DCO-HUA RFS-TSR TRAFFIC FT HUACHUCA AZ//JJJ//
DISA WASHINGTON DC//ISB/ISBE/ISBG/ISBGC//
DISA WASHINGTON DC//D2/D21/D3/D36/D361/D3613/D381//
DISA WASHINGTON DC//D6/JE/JT/WE/WEZ51/WE312//
AIG 8791

UNCLAS

SUBJ/DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS//

REF/A/MSG/DISA WASHINGTON DC/D/121713ZDEC95, SAME SUBJECT//

REF/B/MSG/DISA WASHINGTON DC/D3/182100ZAPR96/SUBJ:DEADLINE EXTENSION

TO DISN SECRET INTERNET PROTOCOL ROUTER NETWORK (SIPRNET) INTERIM NETWORK CONNECTION REQUIREMENTS//
AMPN/REF A ESTABLISHED A DEADLINE FOR SIPRNET SUBSCRIBERS TO MEET SPECIFIC REQUIREMENTS CRUCIAL TO THE OVERALL NETWORK SECURITY OF THE SIPRNET. REF B EXTENDED THE DEADLINE FOR OPERATIONAL SIPRNET CUSTOMERS TO SUBMIT THEIR SYSTEM SECURITY PACKAGES TO 31 JUL 1996.//
POC/TINA HARVEY/MAJ/J6T/LOC:JOINT STAFF/TEL:DSN 223-1747/TEL:COMM (703) 693-1747/EMAIL:HARVEYTM@JS.PENTAGON.MIL//
RMKS/1. IN THE INTEREST OF PROTECTING THE SIPRNET AND ITS SUBSCRIBERS, ALL SIPRNET SUBSCRIBERS THAT DIRECTLY CONNECT TO SIPRNET MUST COMPLETE SYSTEM SECURITY PACKAGES IAW REF A. DISA IS ASSIGNED THE RESPONSIBILITY FOR SIPRNET CONNECTIVITY AND ACCREDITATION AND WILL NOT CONNECT NEW SUBSCRIBERS TO SIPRNET WITHOUT THESE PACKAGES. REF B REQUIRED ALL SIPRNET SUBSCRIBERS HAVE THESE PACKAGES SUBMITTED

TO DISA NLT 31 JUL 96.

2. TO DATE, ONLY 194 OF THE 382 SYSTEMS CURRENTLY CONNECTED HAVE COMPLETED SYSTEM SECURITY PACKAGES. COMPLIANCE IS CRUCIAL FOR ENSURING OVERALL NETWORK SECURITY. TO ASSIST IN COMPLIANCE, JOINT STAFF/J6T MET WITH SERVICE POINTS OF CONTACT ON 10 JAN 97 AND CO-HOSTED A MEETING WITH DISA FOR AGENCIES ON 18 FEB 97 TO AGAIN OUTLINE REQUIREMENTS AND ISSUES. IN ORDER TO DOCUMENT PROGRESS TOWARD RESOLUTION, JOINT STAFF/J6T WILL PERIODICALLY SEND OUT FOLLOW UP MESSAGES TO CINCS, SERVICES AND AGENCIES IDENTIFYING NON-COMPLIANT SYSTEMS UNDER THEIR RESPONSIBILITY.

3. ALL EXISTING SIPRNET SUBSCRIBERS WHO HAVE NOT YET COMPLIED WITH THE REQUIREMENTS IN REFS A AND B MUST CONTACT DISA/D3613 IMMEDIATELY AND SUBMIT SYSTEM SECURITY PACKAGES TO DISA AS OUTLINED IN REF A. DUE DATE FOR ALL PACKAGES CURRENTLY OUTSTANDING IS 15 JUL 97. DISA POCS ARE LISTED IN PARAGRAPH 4 OF THIS MESSAGE. DISA HAS DEVELOPED A PACKAGE THAT PROVIDES DETAILED INSTRUCTIONS AND EXAMPLES OF SYSTEM SECURITY DOCUMENTATION THAT WILL BE MADE AVAILABLE UPON REQUEST. IF SYSTEM SECURITY PACKAGES CANNOT BE COMPLETED BY 15 JUL 97, FORMAL WRITTEN REQUESTS FOR AN EXTENSION ARE REQUIRED. SEND BY MESSAGE TO: DISA WASHINGTON DC//D3613//, BY MEMORANDUM TO: DEFENSE INFORMATION SYSTEMS AGENCY, ATTN: D3613 (JOHN STAPLES), 11440 ISAAC NEWTON SQUARE, RESTON, VA 22090-5087, FAX: DSN 653-8482/COMM 703-735-8482.

REQUESTS FOR EXTENSION MUST INCLUDE: ORGANIZATION POINT OF CONTACT, PROJECTED DATE OF PACKAGE SUBMISSION, ASSIGNED SYSTEM COMMAND AND CONTROL SERVICE DESIGNATOR (CCSD) AND SIPRNET IP ADDRESS FOR EACH DIRECT SIPRNET CONNECTION UNDER THEIR RESPONSIBILITY. APPROVAL WILL BE ON A CASE BY CASE BASIS.
4. RECIPIENTS ARE REQUESTED TO ENSURE WIDEST DISSEMINATION OF THIS MESSAGE. IF THERE ARE ANY QUESTIONS, PLEASE CONTACT DISA/D3613 POCS
A. JOHN STAPLES/DSN: 653-3236/COMM: 703-735-3236/EMAIL STAPLESJ@NCR.DISA.MIL/MAIL: DEFENSE INFORMATION SYSTEMS AGENCY, ATTN: D3613 (MR. JOHN STAPLES), 11440 ISAAC NEWTON SQUARE, RESTON, VA 22090-5087, OR
B. JIM NOSTRANT/DSN: 653-3238/COMM: 703-735-3238/EMAIL: NOSTRANJ@NCR.DISA.MIL//

BT